VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2004 UNIVERSITY OF VIRGINIA VOL. 9, NO. 7

War, Peace, or Stalemate:

Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics

PATRICK S. RYAN[†]

ABSTRACT

A wardriver gets in her car and drives around a given area. Using her laptop, freely available software, a standard Wi-Fi card, and a GPS device, she logs the status and location of wireless networks. The computer generates a file and records networks that are open and networks that are closed. Once the data is collected, the wardriver may denote an open network by using chalk to mark a sign on a building, called "warchalking," or she may record the location on a digital map and publish it on the Internet. This article will explain the roots of the term "wardriving," and the cultural phenomenon of the 1983 Hollywood movie *WarGames* that gave birth to the concept more than 20 years ago. Moreover, this article will show that the press has often confused wardriving with computer crimes involving trespass and illegal access. There are inconspicuous ethical shades to wardriving that are poorly understood, and to date, no academic literature has analyzed the legality of the activity. This article will argue that the act of wardriving itself is quite innocuous, legal, and can even be quite beneficial to society. It will also highlight the need for wardrivers—and for anyone accessing open networks—to help establish and adhere to strict ethical guidelines. Such guidelines are available in various proposal-stage forms, and this article will review these ethics within the context of a larger movement among hackers to develop a coherent ethical code.

[†] Assistant Lecturer and Ph.D. Candidate, Interdisciplinary Center for Law and Information Technology (ICRI), Katholieke Universiteit Leuven, http://www.kuleuven.ac.be/icri. The author studied law at the Universität St. Gallen in Switzerland (MBL-HSG, 2003) and at the University of Texas at Austin (JD, 2000). The author is most grateful to Jos Dumortier for his support and encouragement to write this piece while at ICRI, and to Amon Burton, John Dzienkowski, and Anthony Reese for inspiring me to research further into the intersection of computers and ethics. The author would also like to express his appreciation to the following people who provided feedback on earlier drafts of this piece: Carolyn Daughters, Hans Graux, David Kahn, Wendy McCallum, Phil Weiser, and the VJOLT editorial staff.

TABLE OF CONTENTS

A strange game.
The only winning move is not to play.

W.O.P.R. Computer, a.k.a. "Joshua,"
WarGames (MGM/UA Studios, 1983)

I. INTRODUCTION

¶ 1 The annual Las Vegas hacker's conference known as "DefCon" started in 2002 with a competitive "wardriving" event. Two dozen teams got in their cars and drove through the streets of the city on a Saturday afternoon, scoring points for each unprotected wireless network that they could locate and tap.[1] This competition was repeated in 2003.[2] Wardriving involves first identifying open wireless nodes and then either marking the location of the open nodes on the side of a building with chalk or publishing the location on the Internet. Today, this activity is no longer just for "hackers;" in other words, wardriving has hit the mainstream. The *New York Times* has called wardriving a "grass roots" movement and one of the great ideas of the year.[3] Moreover, the *Frankfurter Allgemeine Zeitung* declared the movement a "national sport" in the United States, and also noted that the practice is quickly moving to Europe.[4] Recently, a how-to wireless-hacking course has been offered at the prestigious Massachusetts Institute of Technology (MIT), promising to teach students how to perform wardriving techniques and how to use "cool wireless tools for [their] tinkering pleasure."[5]

¶ 2 Called "wardriving," "warchalking," and "wireless hacking," this activity takes many forms, some helpful, some innocuous, and some nefarious. The name "*war*driving" is somewhat bizarre—and indeed unfortunate—for the practice has nothing to do with warfare. This article will explain the roots of the unusual term, as well as discuss some of its other forms (*e.g.*, warwalking and warflying)[6] and describe the cultural phenomenon of the 1983 Hollywood movie *WarGames*,[7] which gave birth to the concept more than twenty years ago. In addition, this article will show that the press often confuses wardriving with computer crimes involving trespass and illegal access.[8]

[1] Michelle Delio, *Defcon: A Veritable Hack Fest*, WIRED, Aug. 5, 2002, *available at* http://www.wired.com/news/culture/0,1284,54328,00.html (last visited Jan. 15, 2004) (describing the 2002 DefCon conference and the competition wardrive).

[2] Doug Mohney, *Hackers Wardrive into Wireless,* IWCE, July 1, 2003, *available at* http://iwce-mrt.com/ar/radio_hackers_wardrive_wireless/. For the results of the contest, along with maps of open nodes, see the World Wide Wardrive website, *available at* http://www.worldwidewardrive.org/dc11drive/wardrive.html (last visited Jan. 5, 2004).

[3] Clive Thompson, *The Year in Ideas: War-Chalking*, N.Y. TIMES, Dec. 15, 2002, at 134.

[4] *See* Klemens Polatschek, *Die Zukunft des Hackens ist Drahtlos*, FRANKFURTER ALLGEMEINE ZEITUNG, Feb.10, 2002, at 65.

[5] *See* http://www.mit.edu/iap/2004/wireless/index.html (last visited Jan. 7, 2004). The course is entitled "802.11 Wireless Hacking." The full course description reads as follows: "A technical discussion of the 802.11 MAC layer and how to craft your own wireless frames. This class will also touch on WEP vulnerabilities, *war driving* and insecurities in 802.11 networks and discuss *cool wireless tools for your tinkering pleasure*." *Id.* (emphasis added).

[6] *See* JEFF DUNTEMANN, JEFF DUNTEMANN 'S DRIVE-BY WI-FI GUIDE 371-72 (2003) (noting that "warwalking," common in dense cities like London, Paris, New York, and Washington, D.C. involves the use of a Wi-Fi adapter with a miniature computer such as a PDA, and that "warflying" involves setting up equipment in airplanes; "warbiking" is another common variant).

[7] *WarGames*, MGM/UA Studios, 1983. *See* The Internet Movie Database, *at* http://imdb.com/title/tt0086567 (last visited Dec. 15, 2003).

[8] A man in Canada was caught downloading child pornography on another person's wireless network, and this activity was labelled as being associated with "war driving." See Kim Bradley, Drive-by

There are subtle ethical shades to wardriving that are rarely understood, and to date, no academic literature has evaluated the legality of the activity.

¶ 3 This article will argue that the act of wardriving itself is quite innocuous, that from a legal perspective it is an extension of other activities often referred to as "hacking," and that it can even be beneficial to society. Hacking has become mainstream, as anyone who opens her computer may scan for open networks and log onto them. Wardrivers, hackers, and the general public all need to adhere to strict ethical guidelines. Such guidelines are starting to become available,[9] and this article will review those guidelines within the context of a larger movement among hackers to develop a coherent ethical code. This new movement has gained great momentum in the last few years, and it illustrates the division that separates well-intentioned hackers and members of the general public from others—such as crackers and phreaks—whose intentions are varied and often less benevolent.

A. Wireless Hacking: Scope of the Problem

¶ 4 Since wireless hacking and wardriving are the latest trends in hacking, they will be used to illustrate the scope of the problem. Imagine that a wardriver gets in her car and drives around a given area. Using her laptop, freely available software,[10] a standard Wi-Fi card[11], and a GPS device,[12] she logs the status and location of wireless networks. The computer generates a file and records open and closed networks. Once the data is collected, the wardriver may denote an open network by using chalk to mark a sign on a building, called "warchalking," or she may record the location on a digital map and publish it on the Internet.[13] Once the information is published—either on a building or on an Internet map—other users may go to those locations and access the Internet. At any time, the network owner may close his network by using built-in security measures (*e.g.*, WEP),[14] or he may take steps to install additional firewalls.[15] Or, because his network

Net User Targets Kid Porn, TORONTO SUN, Nov. 22, 2003, *available at* http://www.canoe.ca/NewsStand/TorontoSun/News/2003/11/22/pf-264938.html.

[9] *See* Renderman, *Stumbler Code of Ethics v.0.2*, *available at* http://www.renderlab.Internet/projects/wardrive/ethics.html (last visited Jan. 15, 2004).

[10] Basic wardriving can take place with nothing more than the resident software used to operate a Wi-Fi card. Additional capabilities are also available with specialized programs. S*ee* Steven Levy, *I Was a Wi-Fi Freeloader*, NEWSWEEK, Oct. 14, 2002, at 38 (describing a wardriving program called MacStumbler, used to inform people if they are in the area of other Wi-Fi networks). A related program called NetStumbler features a Web site that includes postings of more than 1,000 articles and other materials on wardriving and wireless security, as well as a $150 wardriving "kit." *See* http://www.netstumbler.com (last visited Jan. 3, 2004).

[11] Wi-Fi stands for "Wireless Fidelity" and is generally considered to be the acronym for the IEEE 802.11b wireless Ethernet standard. *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 825 (2002).

[12] GPS stands for "Global Positioning System," a constellation of twenty-four orbiting satellites that allows the location of devices to be pinpointed within one meter's accuracy. *See id.* at 331-32.

[13] *See* Levy, *supra* note 10.

[14] WEP stands for "Wired-Equivalent Privacy." There have been some concerns with the security levels of WEP, although security has improved greatly in the past couple years. *See* Patrick Mannion, *Cipher Attack Blasts through 802.11 Encryption Scheme, Dealing a Sucker Punch to WLAN Security*, ELEC. ENG'G TIMES, Aug. 6, 2001, at 54 (describing WEP and the development of newer 128-bit encryption keys that are more difficult to penetrate than the older 40-bit keys).

has been "chalked," either on the building walls or on the Internet, he may (perhaps unwittingly) share his network with users who are keen to find free wireless access.[16]

¶ 5 At first glance, wardriving may seem to benefit only those who gain free access to the Internet on open networks. However, the socially advantageous aspects of wardriving are actually rather straightforward: wardriving can alert network users to possible vulnerabilities in their systems so that they may take precautions to protect their data.[17] Wardriving is also appealing to those who would like to share their networks as open nodes for all users, even if such shared use is prohibited by some ISPs.[18]

¶ 6 Wi-Fi and its hacking derivatives present users with a multitude of competing ethics[19] because they bring to light issues surrounding hactivism, open networks, and crime. Federal Communications Commission (FCC) Chairman Michael Powell recently insinuated that people or businesses that wish to share their wireless networks with the public (*e.g.*, coffee shops wanting to attract customers or people who are part of the "open network" movement)[20] should be encouraged to do so: "I challenge all facets of the industry to permit consumers to attach any devices they choose to their broadband connection, so long as the devices operate within service plan limitations and do not harm

[15] *See* Dave Molta, *WLAN Security on the Rise,* NETWORK COMPUTING, Feb. 4, 2002, at 86 (describing various forms of wireless security and firewalls that can be installed to increase security).

[16] *See* Nick Wingfield, *WiFi Moochers*, WALL ST. J., July 31, 2003, at B1 (describing cases where people "mooch" from open, non-secured wireless networks).

[17] Hackers have often been sought out by companies that seek help in finding and troubleshooting security problems and in creating lock-out programs that restrict network access. For example, a company called Rent-A-Hacker, Inc. hires out "hackers" as independent contractors to help companies find and resolve network problems. *See* http://www.rent-a-hacker.com (last visited Jan. 11, 2004). *See also* Jamie Swedberg, *Security in the Real World*, COMPUTERUSER.COM, Nov. 2000, *available at* http://www.computeruser.com/articles/1911,6,31,1,1115,00.html (profiling rent-a-hacker.com and discussing security matters); Dequendre Neeley, *Hire Thine Enemy?*, SECURITY MGMT., Sept. 1, 1999, *available at* 1999 WL 14496643 (noting that many companies hire hackers to conduct "penetration tests" and to offer advice on how to stop others from penetrating their networks).

[18] Internet Service Provider (ISP) contracts do not always permit the sharing of wireless networks. *See* Rachael Metz, *Un-Wired*, PALO ALTO WKLY., Jan. 1, 2003, *available at* http://www.paloaltoonline.com/weekly/morgue/2003/2003_01_01.wireless01.html (interviewing an AT&T Broadband Vice President, who says that customers who share their connections are subject to having their connections terminated as a violation of the company's acceptable use policy); Nick Langley, *The Demise of the Warchalkers*, COMPUTERWEEKLY.COM, June 24, 2003, *available at* http://www.computerweekly.com/Article122783.htm (reporting that AT&T Broadband sent out its own wardrivers to find open wireless access points that may be shared in violation of the terms of its contracts). Not all ISPs prohibit network sharing. For example, the broadband company Speakeasy advertises a "Netshare" product that allows customers to share their Wi-Fi networks with their neighbors. *See* http://www.speakeasy.net/netshare/learnmore/ (last visited Jan. 10, 2004).

[19] The term "cacophony of competing voices" was used by the Supreme Court to describe the FCC rationale for regulation of the wireless spectrum. Red Lion Broad. Co. v. FCC, 395 U.S. 367, 376 (1969) (setting forth the traditional justification for regulation under the 1927 Radio Act: "It quickly became apparent that broadcast frequencies constituted a scarce resource whose use could be regulated and rationalized only by the Government. Without government control, the medium would be of little use because of the cacophony of competing voices, none of which could be clearly and predictably heard.")

[20] *See, e.g.,* The Wi-Fi-FreeSpot Directory, *available at* http://www.wififreespot.com/ (last visited Jan. 22, 2004) (listing free wireless access points all across the United States).

the provider's network or enable theft of service."[21]

¶ 7 In this statement, Powell implicitly (and correctly) assumes that the harmful *derivative* aspects of open Wi-Fi access, wardriving, and wireless hacking are covered by existing law enforcement policies. The derivative by-products include cases involving access to open wireless networks for purposes of downloading child pornography[22] or cases involving anonymous spam sent by companies or individuals.[23] Although the press often associates these problems with wardriving and open Wi-Fi in general,[24] Internet child pornography or anonymous spam via wireless sources should not be classified in the same category.

¶ 8 Unlike wardriving, activities like downloading child pornography and sending spam clearly have no social value in any context, regardless of whether they are performed by means of wired access, wireless access, or in some other manner.[25] Although the proliferation of open wireless standards like Wi-Fi may create more opportunities for anonymous criminal activity, the underlying act remains unchanged. The nature of the criminal activity is not altered by the fact that the criminals are able to cloak themselves behind a wireless mask; the perpetrators remain subject to the law. For example, anti-spam laws vary from country to country[26] and from state to state[27] (and

[21] Michael K. Powell, Remarks at the Silicon Flatirons Symposium on The Digital Broadband Migration: Toward a Regulatory Regime for the Internet Age, presented at the University of Colorado School of Law, at 5 (Feb. 8, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf.

[22] *See* Bradley, *supra* note 8. *See also* Gretchen Drummie, *Alleged "War Driver" Released on $5,000 Bail*, LONDON FREE PRESS, Nov. 25, 2003, *available at* http://www.canoe.ca/NewsStand/LondonFreePress/News/2003/11/25/267415.html (discussing the allegations and the conditions of release on bail of a person caught downloading child pornography and calling him a "war driv[er]").

[23] *See* Steven Levy & Brad Stone, *The Wi-Fi Wave: Rising from the Grass Roots, High-Speed Wireless Internet Connections are Springing up Everywhere*, NEWSWEEK, June 10, 2002, at 38 (describing network vulnerabilities of wardriving and the problems that can occur, such as spam being sent by a wardriver); George Cho, *Drive-By Spam: A New Form of Freedom of Expression; War-driving and War-chalking for Fun and Profit*, CANBERRA TIMES, Sept. 30, 2002, at 15 (describing the practice of using unprotected wireless networks to send spam in London and elsewhere); Saul Hansell, *Virginia Law Makes Spam, with Fraud, a Felony*, N.Y. TIMES, Apr. 30, 2003, at C1 (describing a Virginia law that criminalizes fraudulent, high-volume, and anonymous spam).

[24] *See* Jennigay Coetzer, *Hackers will Mark Victims' Premises,* BUS. DAY (South Africa), July 22, 2003, at 14, (describing wardriving and wardrivers, labeling wardrivers "hackers," and warning of security breaches made by wardrivers); *Warchalkers Make Mark in Latest Hacking Craze*, BIRMINGHAM POST (U.K.), Aug. 5, 2002, at 32 (describing wardriving and warchalking and calling all wardrivers "hackers"); *Men Charged with Hacking National Chain's System*, GRAND RAPIDS PRESS, Nov. 11, 2003, at D5 (describing hackers who hacked into a Lowe's computer system as having been "engaged in 'wardriving'"; this criminal case is discussed further in Section IV, *infra*).

[25] The Child Pornography Prevention Act (CPPA) of 1996 contains federal prohibitions on child pornography and criminalizes the act of viewing child pornography, regardless of the medium through which it was obtained. *See* 18 U.S.C. § 2256 *et seq.* (2004).

[26] For an overview of applicable anti-spam laws in the European Union and in other countries, see David E. Sorkin, *Spam Laws*, *available at* http://www.spamlaws.com (last visited Jan. 10, 2004).

[27] For an overview of the applicable anti-spam laws passed in the individual U.S. states, see *id*.

often are contractual or tort matters[28]), but generally they apply to any transmission format. Child pornography is also universally criminal,[29] regardless of when, where, or how it takes place.[30]

¶ 9 There is a widespread assumption that wardriving is legal. One website even proclaimed its legality by selling t-shirts and other items promoting wardriving.[31] Indeed, the commercial motivations for proclaiming wardriving legal seem to be very strong, as many websites that discuss the activity also sell something, such as consultancy services, security equipment, or both.[32] The premise that wardriving is legal relies on a narrowly construed and somewhat arcane distinction between *viewing* or *recording* the existence of open networks and *accessing* those networks.[33] The criminality of wardriving remains to

[28] Spam is often prohibited by service agreements that exist between users and ISPs. *See, e.g.,* MonsterHut, Inc. v. PaeTec Communications, Inc., 741 N.Y.S.2d 820 (N.Y. App. Div. 2002) (Internet service provider terminated a contract because a subscriber sent spam in breach of the agreement).

[29] *See, e.g.*, United States v. Adams, 343 F.3d 1024, 1032 (9th Cir. 2003) (describing the U.S. legislative history and Congressional intent with regard to child pornography laws:

> Legislative history leads us to three observations: (1) Congress determined that child pornography is a multi-million dollar industry in which sexually explicit depictions of children are bought, sold, and traded interstate; (2) Congress decided to "stamp out" the market for child pornography by criminalizing the production, distribution, receipt, and possession of child pornography; and (3) Congress thought it could strike a blow to the industry by proscribing possession of child pornography "because those who possess and view child pornography encourage its continual production and distribution. (citations omitted)).

[30] It should be noted, however, that an exception to child pornography is the recent "virtual child pornography" decision, which holds that animations are protected by the First Amendment. Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). The Child Pornography Prevention Act of 1996, 18 U.S.C. § 2256(8)(B), prohibits "any visual depiction, including any film, video, picture, or computer or computer-generated image or picture" that "is or appears to be of a minor engaging in sexually explicit conduct." In *Free Speech Coalition*, the Supreme Court held, *inter alia,* that § 2256(8)(B) was overbroad and unconstitutional. 535 U.S. at 258. *See generally* Alice G. McAffee, Note, *Creating Kid-Friendly Webspace: A Playground Model for Internet Regulation*, 82 TEX. L. REV. 201 (2003) (describing the history of child pornography legislation in the United States, *Ashcroft v. Free Speech Coalition*, and additional issues related to Internet child pornography).

[31] The website http://www.wardrivingisnotacrime.org appears to have gone inactive sometime during the last week of December 2003 (archived copy on file with author). *See also* Mike Wendland, *Wardrivers Say Idea is to Find Networks, not Steal*, DETROIT FREE PRESS, Nov. 14, 2003, *available at* http://www.freep.com/money/tech/mwend14_20031114.htm (discussing the non-criminal claims of wardrivers and citing the existence of the—apparently now defunct—website http://www.wardrivingisnotacrime.org); Tony Bridges, *Encryption Equipment a Priority for Wireless Users*, TALLAHASSEE DEMOCRAT, Nov. 23, 2003, at A2 (discussing wardriving and referring readers to http://www.wardrivingisnotacrime.com.)

[32] *See* William M. Bulkeley, *Hackers' Assault on Networks Is Market Opportunity,* WALL ST. J. EUR., Oct. 24, 2002, at A11 (noting that major companies such as IBM, KPMG, and security firm Guardent, Inc. benefited by marketing and selling additional security devices in the range of $15,000 to $30,000 to protect people from an organized "world-wide 'war drive'"). *See also* Tyler Hamilton, *Insecure Wireless Networks Exposed,* TORONTO STAR, Sept. 10, 2002 (discussing the website http://www.nakedwireless.ca and commercial interest in Canadian companies that sell security services).

[33] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) (a comprehensive article discussing the problems of distinguishing the meaning of the terms *authorization* and *access* in several computer-related criminal statutes).

be tested in the courts. At this time, there are no public wireless cases or settlements indicated on the U.S. Government's computer-crime website.[34] Nevertheless, there have been wardriving-related prosecutions, with undoubtedly more to come in the future (see Section IV, below).

B. Hollywood Roots: WarGames

¶ 10 In order to understand where wardriving came from and where it is headed, it is useful to review its Hollywood roots. The term and the practice of wardriving descend from the 1983 cold-war thriller *WarGames*, in which young Matthew Broderick plays David Lightman, a teenage hacker who wreaks havoc on the U.S. defense system. This movie has become something of a cult phenomenon in hacking circles and has been discussed in several law review articles and other literature on cyber-criminality.[35]

¶ 11 Lightman's actions in the movie are unethical and even illegal, even if many of those same actions can be attributed to adolescent naïveté. Many say that the character is based on real-life hacker Kevin Mitnick, which, if true, underscores the character's underlying criminal motives.[36] In the movie, Lightman begins by breaking into the school's computer system and changes his Biology grade from an "F" to a passing grade. Next, he decides to hack into a computer company's system to download (steal) and play video games on his computer. Accordingly, he develops a computer program that scans phone area codes and prefixes for computer "carrier tones." The program works like this: when a person answers the phone, the computer hangs up and moves on to the next number sequence. When the program detects another computer, it logs it separately so that Lightman can come back later and "hack" into the system. Although not labeled as

[34] *See* Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Computer Intrusion Cases, *available at* http://www.usdoj.gov/criminal/cybercrime/cccases.html (last visited Jan.. 5, 2004).

[35] *See* Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 175-78 (2000) (describing the "*WarGames* Stereotype" of a young, white, male student hacker and pointing to the influence that the movie had in 1980s lawmaking); Kerr, *supra* note 33, at 1641 n.208 (briefly discussing the *WarGames* scenario in the context of describing wardialing); Marc D. Goodman, *Why the Police Don't Care about Computer Crime*, 10 HARV. J.L. & TECH. 465, 469-70 (1997) (discussing the stereotypical hacker, referring to *WarGames*, and incorrectly describing Broderick's character, David Lightman, as an "innocent."). As will be discussed below, Lightman intends to download and steal a game, which cannot be considered an innocent act; a white-collar act, perhaps—because no one is physically injured—but certainly not an innocent one.

[36] Kevin Mitnick is widely recognized as one of the world's most notorious hackers, and he has spent many years in jail. While he denies having hacked into the North American Aerospace Defense Command (NORAD), many hackers credit him as the inspiration for Broderick's character in WarGames. The Mitnick story has been the subject of a best-selling novel and numerous articles. *See* TSUTOMU SHIMOMURA & JOHN MARKOFF, TAKEDOWN: THE PURSUIT AND CAPTURE OF KEVIN MITNICK, AMERICA'S MOST WANTED COMPUTER OUTLAW-BY THE MAN WHO DID IT (1996). A website dedicated to *Takedown* is also available at http://www.takedown.com (last visited Jan. 10, 2004). *See also* Adam L. Penenberg, *Mitnick Speaks!,* FORBES.COM, Apr. 5, 1999, *available at* http://www.forbes.com/1999/04/05/feat.html (last visited Jan. 12, 2004) (an interview with Kevin Mitnick, describing his hacking history, his ties with war games, and his denial of ever having hacked into NORAD); Michelle Delio, *The Greatest Hacks of All Time*, WIRED.COM, Feb. 6, 2001, *available at* http://www.wired.com/news/print/0,1294,41630,00.html (labeling Mitnick as one of the greatest hackers of all time).

such in the movie, in hacking circles this program would later be called a "wardialer."

¶ 12 Subsequently, the young hacker sets up his phone to make long-distance calls that bypass toll charges.[37] After a couple of days of dialing, he finds a game, logs in as the Root user ("Joshua," a login reserved for the original programmer), and plays a game called "Global Thermonuclear War." Later, he discovers by watching the news that the U.S. government fears a Soviet attack. As it turns out, the "game" that Lightman had been playing is really a U.S. military computer called W.O.P.R. (War Operation Plan Response) used for war simulations and war games. By means akin to *Terminator*-esque artificial intelligence, W.O.P.R. learns how to control the nuclear arsenal. For the computer, Global Thermonuclear War is not just a game. W.O.P.R. begins playing the thermonuclear scenario for real, and it initiates a loop that later acquires codes to launch real missiles against Soviet opponents. A thrilling countdown begins: the race is on as W.O.P.R. locks out human programmers and begins to decipher the launch codes.

¶ 13 Happily, the world is ultimately saved by young Lightman, who "teaches" the computer the futility of nuclear war by forcing it to play itself in a rapid-fire game of tic-tac-toe, a game that always ends in a tie. Lightman joins forces with the original programmer, who hopes that W.O.P.R. applies what it has learned from tic-tac-toe to global thermonuclear warfare. In the final seconds, W.O.P.R. announces (in a 1980s-style computer voice) that nuclear war is "[a] strange game. The only winning move is not to play." The computer thus releases its control of the nuclear arsenal and the world is safe again.

¶ 14 *WarGames* fantastically captured many Americans' fears of imminent nuclear war, and it prophetically depicted people's anxiety about personal computers. The movie also taught an important lesson to programmers who were quickly learning that they must block access to vulnerable electronic backdoors. *WarGames* was even credited in federal legislation for why laws must be passed to curtail computer crimes by acknowledging that the hacking activity depicted in *WarGames* provided a "realistic representation" of hacking and computer access problems.[38]

¶ 15 In fact, derivatives of the *WarGames* scenario still play out today with similar haunting concerns: companies are still worried that hackers will break into systems (now using wireless networks as another means of entry) and steal trade secrets, just as Lightman hoped to do when he thought he was downloading games from a private company.[39] Indeed, trade secrets can be extremely valuable. In one case, computer

[37] In the movie, Lightman's girlfriend comments on the expense involved in making long-distance phone calls, and he replies that "there are ways around that;" however, the manner in which Lightman bypasses toll charges is not detailed in the movie.

[38] H.R. REP. NO. 894, at 10-11 (1984) (legislative history to the Counterfeit Access Device and Computer Fraud and Abuse Law, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190 (1984)). The legislative history states: "The Motion Picture 'WarGames' showed a realistic representation of the automatic dialing and access capabilities of the personal computer"). *See also* Calkins, *supra* note 35, at 175-77 (noting the influence of *WarGames*, the hacker stereotypes that it created, and its ongoing influence on public perceptions of hackers).

[39] *See* Pavlovich v. Superior Court, 58 P.3d 2 (Cal. 2002). In this case, Pavlovich worked on defeating DVD copy protection and put up a webpage with information about the Decryption of Contents

hackers broke into a company called Interactive Television Technologies and stole technology secrets worth $250 million, thus putting the company out of business.[40]

¶ 16 Theft of trade secrets is certainly a concern in 2004. Likewise, various forms of terrorism (*e.g.*, nuclear[41] and computer-related[42]) are also growing areas of anxiety. The U.S. government even issued a special warning that wardriving could be used by terrorists, noting that "[a] person driving in a car around a city, for example, can access many wireless local area networks without the knowledge of their owners unless strong security measures are added to those systems."[43] While these capabilities do indeed exist, such statements do little more than feed the public's continued paranoia over legitimate derivative uses for personal computers. One can easily imagine that if a *WarGames* sequel were made in this decade, the plot might involve wireless hacking to steal government or corporate trade secrets or involve use of jamming devices to disrupt other forms of wireless communications that have emerged since 1983 (*e.g.*, mobile phones, cordless phones, Wi-Fi, baby monitors, and Bluetooth connections). In the two decades that have passed since the release of *WarGames*, the world has become wireless,[44] and access to the airwaves has opened up new opportunities for crime and terrorism.

II. WARDIALING

¶ 17 Many of the new opportunities for crime are still based on older, fairly well-known acts such as "wardialing." Beginning in the mid- to late-1980s, groups of kids,[45] cyber-heroes (often doubling as security entrepreneurs),[46] and criminals[47] built upon the

Scrambling System (DeCSS) program. A DVD association brought suit against Pavlovich based only on the existence of his website in California, alleging that he had "misappropriated its trade secrets." *Id.* at 6. The court ultimately found that California had no personal jurisdiction over Pavlovich. *Id.* at 13.

[40] *See Industrial Espionage Victimizes Company of Revolutionary Internet Technology Worth $250 Million,* PR NEWSWIRE, Aug. 16, 1996; Jon Swartz, *Modern Thieves Prefer Computers to Guns/Online Crime Is Seldom Reported, Hard to Detect*, SAN FRANCISCO CHRON., Mar. 25, 1997, at A1.

[41] *See Could Worse Be Yet to Come?*, ECONOMIST, Nov. 3, 2001, at SR1 (describing frightening scenarios where terrorists use nuclear weapons).

[42] *See Fighting the Worms of Mass Destruction,* ECONOMIST, Nov. 29, 2003, at 76 (noting widespread fears of cyber-terrorism and describing an event in Australia where a terrorist broke into computers in an Australian sewage treatment plant and rerouted sewer contents into a freshwater source).

[43] *See The National Strategy to Secure Cyberspace*, Feb. 2003, at 35, *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf. *See also* Paul Boutin, *Feds Label Wi-Fi a Terrorist Tool*, WIRED, Dec. 6, 2002, *available at* http://www.wired.com/news/wireless/0,1382,56742,00.html (describing problems with wireless security and government measures warning of terrorists' use of wireless technology).

[44] Jonathan Krim, *WiFi Is Open, Free and Vulnerable to Hackers*, WASH. POST, July 27, 2003, at A1 (noting that a report from Gartner, Inc. estimates that last year there were 3.1 million U.S. households with wireless networks and that there will be as many as 75 million users of hot spots by 2008).

[45] *See* Jason Tudor, *ID Theft Provides Valuable Lesson in Holiday Caution,* U.S. AIR FORCES IN EUROPE NEWS SERVICE, Dec. 19, 2003, *available at* http://www.dcmilitary.com/airforce/beam/8_50/commentary/26798-1.html (the author describes his own experience in wardialing in his youth using a Commodore Vic-20).

[46] One of the best-known researchers in this area is Peter Shipley, who invented the term "wardriving" and who has published several studies on wardialing. *See* http://www.dis.org/shipley/ (last visited Jan. 3, 2004). *See also* Lee Gomes, *Silicon Valley's Open Secrets*, WALL ST. J., Apr. 27, 2001, at

WarGames legacy and coined a new term—and game—called wardialing.[48] Software for wardialing quickly became available on Apple and (the then very popular) Commodore computers.[49] Like young Lightman in *WarGames*, many wardialers were smart hackers with varied intentions. To predict how war*driving* may be handled by courts and legislators, it is useful to review how its predecessor, war*dialing*, has been dealt with by lawmakers and courts.

¶ 18 For purposes of elucidation, we begin with an overview of the practice of wardialing. A wardialer sets up her computer to dial all numbers within certain area codes and prefixes. The program automatically accesses and records basic information from the numbers that they dial, such as whether the call is answered by a person, a computer, or a fax machine. When computers answer, the programs record the information that these computers freely give them, such as the answering computer's identification information. In more complicated scenarios, computer programs automatically attempt to generate passwords.[50] Wardialers, like others in the hacking community, compile databases of this information for personal use or to post it publicly, either on "bulletin boards"[51] or, more recently, on the Internet.[52]

¶ 19 Hackers make this information available to anyone who is interested. Popular

B1 (interviewing Shipley during a wardrive and emphasizing that he and his colleagues "aren't malevolent hackers . . . their aim is utterly benign: to expose one of the newest and potentially most dangerous securities holes in U.S. business, in the form of wireless computer networks"). *See also* William M. Bulkeley, *Hacker Assault on Networks Is Chance for Sales,* WALL ST. J., Oct. 23, 2002, at B1 (crediting Peter Shipley with the invention of wardriving and noting that its purpose is driven by the marketing interests of computer security firms that embarrass companies and sell them services).

[47] *See* David L. Gripman*, The Doors are Locked but the Thieves and Vandals are Still Getting in: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem,* 16 MARSHALL J. COMPUTER & INFO. L. 167*,* 168 n.6 (1997) (describing a wardialing scenario where hackers attempt to break into a computer system and steal information); Jennifer Alvey, *Digital Terrorism: Hole in the Firewall?* 140 PUB. UTIL. FORT. 12 (Mar. 15, 2002) (describing security problems, discussing the wardialing phenomenon, and quoting from a Rush Limbaugh transcript where the topic was covered in some detail. *Id.* at 18-19).

[48] *See* Richard Behar, *Who's Reading Your E-Mail? As the World gets Networked, Spies, Rogue Employees, and Bored Teens are Invading Companies' Computers to Make Mischief, Steal Trade Secrets – Even Sabotage Careers*, FORTUNE, Feb. 3, 1997, at 56 (describes the growth of hacking and a detailed scenario of the invasion of a Fortune 500 company, including the practice of using wardialing software to break into computer "back doors").

[49] *See id.* (describing the functionalities of a wardialing program called ToneLoc).

[50] *See* State v. Riley, 846 P.2d 1365, 1367-68 (Wash. 1993) (defendant was charged and sentenced for computer trespass. The defendant set up his computer to automatically dial a telephone company's computer every fifty seconds and to hack into the company's system by attempting to enter six-digit access codes).

[51] *See Writer Feels Wrath of Computer Buffs Angered by Article,* N.Y. TIMES, Dec. 9, 1984, at 88 (describing problems encountered by a NEWSWEEK reporter whose Visa credit card account number was posted on bulletin boards after he wrote a story that criticized hackers; the short article also captured the beginning of "hacking" concerns, quoting a Stanford researcher: "[t]he problem has been in not taking hackers seriously … [b]ut that perspective is changing").

[52] *See, e.g.*, State v. Brown, 2004 WL 27207, at *5 (Wash. App. Div. 2004) (unpublished decision). *Brown* is a criminal case on identity theft. Evidence included saved Internet webpages on the defendant's computer that showed information about how to change identities and create false credit cards, as well as other information on committing crimes. *Id.*

hacking websites include 2600.com,[53] which publishes a periodical called *The Hacker Quarterly*.[54] Detailed information on how to hack can be obtained from other sources, such as the Internet publication *Phrack*.[55] These sites may alarm some people, since they detail security loopholes. However, their open publication of hacking material also helps security experts develop better ways to protect networks.[56]

¶ 20 In support of the argument that some aspects of wardialing and hacking constitute a public service and provide a social benefit, one scholar has proposed "hack-in contests" as a means to derive a tangible social value from hackers' capabilities and efforts.[57] However, such proposals are better in theory than in practice. Hacking contests with only one or two winners have not been well received by the hacker community because many hackers refuse to spend time on a project if they are paid only if they win.[58] In one famous case, a Princeton computer science professor accepted a hacking challenge—and won—but refused to sign the confidentiality agreement (a condition of the prize), instead choosing to publish the results of his efforts.[59] His actions greatly frustrated the sponsoring company, which found unexpected support from the Recording Industry Association of America (RIAA), an industry lobby group that is now (in)famous for suing hackers of all ages and other controversial practices.[60] Ultimately, the matter was

[53] The name "2600" was chosen because phreaks used 2600 hertz tone to gain unauthorized access to telephone networks through the various "boxes" described below in Section III. The first phreaking "box" has in fact been attributed to a toy whistle that came from a Captain Crunch cereal box that, when blown, emitted a 2600 Hertz signal. *See* Delio, *supra* note 36 (attributing the 2600 Hertz tone and discovery of its effect on telephone networks to John Draper and telling the "cereal box" story; Draper also was well known in the hacker community by his alias "Captain Crunch" because the whistle came out of a Captain Crunch cereal box). *See also* Universal City Studios, Inc. v. Reimerdes*,* 111 F. Supp. 2d 294, 308 (S.D.N.Y. 2000) (noting the origins of 2600.com as publisher of THE HACKER QUARTERLY, which was also one of the defendants in the case).

[54] *See* http://www.2600.com/ (last visited Jan. 7, 2004).

[55] *See* http://www.phrack.org/ (last visited Jan. 7, 2004). The term "phrack" was invented by merging the terms "phreak" and "hack." *See* Dorothy E. Denning, The United States vs. Craig Neidorf*: A Viewpoint on Electronic Publishing, Consitutional Rights, and Hacking*, 34 COMMS. OF THE ACM 24 (1991), *available at* http://www.cs.georgetown.edu/~denning/ infosec/Neidorf.txt.

[56] 2600 Enterprises, Inc., the publisher of 2600.com and *The Hacker Quarterly*, was also subject of a lawsuit involving its publication of details on the DVD core code. Per court order, the company was required to remove this information from its website. *See* Reimerdes, 111 F. Supp. 2d at 306. The order is also available at http://www.2600.com/dvd/docs/2000/0817-order.pdf (last visited Jan. 7, 2004).

[57] *See* Brent Wible, Note, *A Site Where Hackers Are Welcome: Using Hack-in Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L.J. 1577 (2003).

[58] In 2000, the Secure Digital Music Initiative (SDMI) offered a prize of $10,000 to any hacker who could crack its program. Most hackers refused, protesting that their efforts would amount to "free consulting" because they would be paid nothing for their time. Unlike hackers, who are only paid when they win such contests, commercial consultants are paid hourly for their efforts. *See To Hack, or Not to Hack?,* ECONOMIST, Sept. 21, 2000.

[59] Edward W. Felten et al., *Reading Between the Lines: Lessons from the SDMI Challenge*, PROC. OF THE 10TH USENIX SEC. SYMP. (2001), *available at* http://www.usenix.org/publications/ library/proceedings/sec01/craver.pdf (last visited Jan. 31, 2004) (publishing the results of the SDMI challenge; footnote 1 states that the authors refused to sign the confidentiality agreement and instead chose to retain the right to publish the paper).

[60] The RIAA has sued minors and senior citizens, and many of these suits have been highly controversial because hackers and the public believe that they should have a right to freely share music and files, and because some of the unhappy targets have been very old or very young. For example, the RIAA

settled between the professor and the company, but not before RIAA realized that it had awoken the fury of a large coalition of respected scientists, academics, and corporations that vehemently supported the professor's position.[61]

¶ 21 In short, both the RIAA and the company that sponsored the contest made a grave public relations error and demonstrated a gross disconnect with academics, hackers, and the general public. As is very common with university research, the aforementioned coalition saw the contest as an express invitation to hack the sponsoring company's product. In a natural extension of this idea, these individuals foresaw no barriers to disclosure of the system's vulnerabilities, especially since research (here hacking) and publication of the results is exactly what scientists and academics do without impediment every day. Although the sponsoring company undoubtably found $10,000 a fair exhange for a confidential report on problems within its encryption system, the professor clearly valued the opportunity to publish the results of his efforts more than the prize money. Despite this incident, however, hack-in contests continue, and there will probably always be a place for them as long as the value proposition makes sense to both hackers and those who openly request that their systems be hacked.[62]

¶ 22 Nevertheless, it is unlikely that hack-in contests will gain widespread popularity. Instead, it is more probable that hackers will continue to find work as project-based hourly consultants. For example, on several recent occasions federal and state governments employed hackers on an hourly or project basis to test the integrity of new electronic voting systems. A fascinating NPR report details how a hacker hired by the Commonwealth of Maryland unlocked a voting terminal and wardialed into the state's mainframe computer.[63] To prevent such a scenario from occurring outside of a test environment, the election officials placed a special tamper-proof tape on the terminal that would signal tampering.[64] The federal government has also purchased the consulting services of several hackers to test the integrity of the controversial new electronic voting

sued senior citizen Sara Ward and a 12-year old girl. There have also been multiple suits on college campuses and elsewhere. While many suits have been for legitimate infringements, others have come under extreme scrutiny. *See Online Music Update*, 5 E-COM. L. REP. 9 (2003) (describing various suits against campuses and the withdrawal of the lawsuit against Sara Ward); Michael D. Scott, *Wanted: a New Game Plan for the Recording Industry*, 8 CYBERSPACE LAW 1 (2003) (describing the RIAA's suit against a 12-year old girl and calling for a change in strategy).

[61] *See* Press Release, Electronic Frontier Foundation, Princeton Scientists Sue over Squelched Research, *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/ 20010813_eff_felten_pr.html (Aug. 13, 2001) (describing the challenge and providing additional background information and hyperlinks regarding the dispute).

[62] Sometimes the value proposition is a financial one, as discussed above. In other cases, such contests are purely malicious. For example, in July 2003 a contest entitled "The Defacers Challenge," was announced, and involved a race to see which computer hacker could be the first to deface six thousand websites within a six-hour period on July 6, 2003. The contest was reportedly closely watched by the FBI. *See* Keith Regan, *Web Sites on Alert for Hacker Contest*, ECOMMERCETIMES.COM, July 3, 2003, *available at* http://www.technewsworld.com/perl/story/21771.html (describing pre-contest concerns and alerts). *See also* http://www.defacers-challenge.com (a website that uses an unusual *WarGames*-type green font and that states "the challenge not over, im coming back" [sic]).

[63] *All Things Considered: Hackers Help Test Voting Machines* (NPR radio broadcast, Jan. 29, 2004), *available at* http://www.npr.org/rundowns/segment.php?wfId=1624506.

[64] *Id.*

system and to ensure that it is safe from external wardialing and other forms of hacking.[65] In fact, there is a rapidly developing commercial hacking enterprise (see discussion further in Section VI, below).

¶ 23 Returning to the broader discussion of wardialing, it should be emphasized that wardialers are not unlike self-appointed neighborhood watchmen who police an area looking for security breaches. So long as the well-intentioned watchmen do not take advantage of the security breaches they discover, no crime is committed. Moreover, it is reasonable to assume that most, if not all, of those living in the neighborhood are thankful to have watchmen patrolling the area.[66] The difference is that wardialers seem more like bogeymen, because they shock network owners, as would watchmen who open their neighbors' doors while shouting "we're here!" Other analogous situations highlight similar ethical dilemmas. For example, on several occasions, apparently well-intentioned airline employees have breached airport security on their own initiative in order to demonstrate security holes.[67] Though shocking and troubling to many, such actions undoubtedly precipitate appropriate remedies to serious problems.[68]

¶ 24 The hiring of hackers by the government demonstrates that the public can benefit from wardialers' experience and learn to protect themselves from those who possess devious motives.[69] It is important to note that we are dealing with fringe activities; after all, hackers do steal copyrighted broadcasts[70] and other files,[71] appropriate trade secrets,[72] and "lock out" users from corporate voice mail systems.[73] Hackers who commit crimes

[65] *See* Peter Loftus, *Accenture Tackles the Challenges of Electronic Voting, Registration*, WALL ST. J., Jan. 14, 2004, *available at* 2004 WL-WSJ 56917065 (noting that the Defense Department is using its own experts to "hack into [the voting] system," and test its integrity and discussing various security contracts with consulting firms like Accenture and others).

[66] The United States Neighborhood Watch Program is associated with the National Sheriffs' Association and is highly organized. The organization has existed for several decades and is very respectful of privacy issues. *See* http://www.usaonwatch.org (last visited Feb. 5, 2004).

[67] Blake Morrison, *Workers Breach Airport Security*, USA TODAY, April 24, 2002, *available at* http://www.usatoday.com/news/nation/2002/04/24/security-lapse.htm (reporting that there were "at least two dozen incidents of improper behavior or deliberate attempts to bypass security by airline, airport or government workers").

[68] *See* Stephen Power, *Effort to Protect Travelers Hits Turbulence*, WALL ST. J., May 22, 2002, at A4 (describing the many known vulnerabilities at airports and the federal government's efforts to overhaul the system).

[69] The type of facility may be relevant. Accessing the computers of a bank may be different than accessing the computers of a home. *See* People v. Davis, 958 P.2d 1083, 1088 (Cal. 1998) (noting that under the California burglary statute a defendant who accesses a bank's computer from her home using her computer and a modem has electronically entered the bank building and arguably committed burglary).

[70] *See, e.g.,* United States v. Manzer, 69 F.3d 222 (8th Cir. 1995) (hacker convicted of fraud for stealing copyrighted broadcasts).

[71] *See* United States v. Riggs, 739 F. Supp. 414, 416-17 (N.D. Ill. 1990) (court upheld indictment on charges of wire fraud and other crimes for theft of a Bell South text file containing 911 codes).

[72] Cases involving the Church of Scientology and its efforts to protect its trade secret rights in scriptures also illustrate how trade secret rights can be lost over the Internet. *See, e.g.*, Religious Tech. Ctr. v. Lerma, 897 F. Supp. 260, 261-62 (E.D. Va. 1995); Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 901 F. Supp. 1519, 1521-22 (D. Colo. 1995); Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1364-65 (E.D. Va. 1995).

[73] *See* Commonwealth v. Gerulis, 616 A.2d 686, 691-93 (Pa. Super. Ct. 1992), *appeal denied*, 633 A.2d 150 (1993). The court held that accessing a "voice mailbox" was a computer-related crime because

should be punished. But that does not change the fact that *dialing* is not a crime unless the caller does something additional to *access* the computer system itself, thereby committing a crime treated by appropriate laws.[74]

¶ 25 It is not a mental stretch to differentiate wardialing from unauthorized computer access. Many states have passed statutes criminalizing "computer trespass," an act analogous to burglary that involves more than just dialing: it requires an "intent to commit another crime."[75] Recall that common law burglary is the breaking and entry of the dwelling of another at night *with the intent to commit a crime therein.*[76] Therefore, intent is key. With a few notable exceptions, wardialers have been free to pursue their endeavors so long as they stay on the right side of the law.[77]

III. PHREAKING

¶ 26 Another phenomenon that is often associated with wardialing—but that is completely separate from it—is "phreaking." Phreaking involves hackers or "crackers"[78]

the mailbox was created by a computer and messages in the mailbox were stored on computer disks. The defendant used a telephone to access computer-generated voice mailboxes. She then entered data into the mailboxes and changed the password for each so that the authorized users could no longer gain access to them. It was the defendant's manipulation of the voice mailbox (not the mere use of the telephone) that violated the Pennsylvania statute. *Gerulis*, 616 A.2d at 691-93.

[74] *See* State v. Allen, 917 P.2d 848, 850-54 (Kan. 1996). The court interpreted a state computer crime statute, K.S.A. 21-3755—where access is required for a crime to be committed—and held that a defendant does not gain "access" to a computer system merely by dialing a telephone number answered by a computer. To gain access, the defendant must penetrate any security devices in order to gain the ability to use the computer or obtain data from its memory. *Id.*

[75] *See, e.g.,* WASH. REV. CODE ANN. § 9A.52.110 (2004). *See also* State v. Riley, 846 P.2d 1365 (Wash. 1993) (prosecution of computer trespass under § 9A.52.110).

[76] *See e.g.,* State v. Frazier, 389 N.E.2d 1118, 1120 (Ohio 1979) (discussing common-law burglary and noting that it is irrelevant whether the crime after breaking and entry is in fact committed, reiterating that it is the *intent* to commit a crime that gives rise to burglary charges).

[77] One of the more famous exceptions is the case of David McOwen, a PC specialist employed by Georgia's DeKalb Technical Institute who was charged with participating in a distributed computing project run by a non-profit organization that allowed computer users to donate their unused processing power to test the strength of a certain type of encryption. Berkeley made distributed computing famous through its SETI Program. *See* http://www.seti-inst.edu. McOwen installed the distributive computing program on university computers, and the computing power was then used for hacking purposes (without McOwen's direct involvement). As a result, McOwen was charged with computer trespass and faced the possibility of 120 years of jail and a fine of $415,000. *See* Andy Patrizio, *Distributed's New Word: Please*, WIRED.COM, Jan. 24, 2002, *available at* http://www.wired.com/news/technology/0,1282,49961,00.html. Ultimately, he struck a probation deal with the prosecutors. *Id.* A popular website was created in support of McOwen. *See* http://www.freemcowen.com (last visited Dec. 15, 2003). *See also* Evan Hansen, *When Misguided Plans Go from Bad to Worse*, CNET.COM, Aug. 7, 2001, *available at* http://news.com.com/2010-1071-281530.html?legacy=cnet&tag=bt_pr.

[78] This article will not go to great lengths to differentiate these terms. Generally speaking, however, "hackers" vehemently oppose the association of the term "hacking" with crime or malfeasance. Instead, they prefer use of the term "crackers" to describe those who break codes with the intention to commit crimes. *See* Eric S. Raymond, *How to Become: A Hacker,* OREILLY.COM, *available at* http://www.oreillynet.com/pub/a/oreilly/hacks/news/0103_raymond.html (last viewed July 1, 2004).

making phone calls for "phree"[79] by tricking the telephone system. Given phreaks' willingness to break the law, it is not surprising that they also download private data, share copyrighted files, and commit fraud and other felonies such as the dissemination of calling-card and credit-card numbers.[80] Lightman also uses phreaking techniques to make various phone calls in *WarGames*, although his actions are not labeled as such.[81] Many of these crimes are not new; rather, it is the *widespread availability of information* that is new, making the crimes of theft and fraud easier to commit. Indeed, many courts consider phreaking to be theft of telephone services or fraud.[82] Phreaks are also adept at hiding criminal material (*e.g.,* child pornography) in secret, "off-Net" areas.[83] In such cases, the material is accessible to small groups of individuals who know where to locate it and who often have criminal intentions.[84]

¶ 27 Phreaking preceded computer hacking—probably by several years or even decades—since ways of bypassing the phone system existed before the widespread use of personal computers.[85] Some, like Bruce Sterling, also assert an important behavioral distinction between phreaking and hacking. He notes that "hackers are intensely interested in the 'system' *per se*, and enjoy relating to machines. 'Phreaks' are more social, manipulating the system in a rough-and-ready fashion in order to get through to other human beings, fast, cheap and under the table."[86] In most cases, phreaks are treated as criminals, and when caught, they are punished for the services that they steal. To ensure that theft is punished, legislators have tightened the legal chokehold by bringing

[79] The substitution of "ph" for "f" is often used to indicate the illegal use of phones. *See Fighting the Worms of Mass Destruction,* ECONOMIST, Nov. 29, 2003, at 76 (describing "phishing" as the tricks that some use to get recipients to give out sensitive information, such as credit-card numbers).

[80] *See, e.g.,* Commonwealth v. Gerulis, 616 A.2d 686, 697-99 (Pa. Super. Ct. 1992) (citing the trial-court transcript of a "phreaker" who shared illegal calling-card numbers with others).

[81] As noted briefly *supra* note 37, Lightman makes long-distance calls at no charge. Later, while running from the FBI, Lightman uses a hotwiring technique to allow him to call his girlfriend from a payphone at no cost.

[82] *See* United States v. Henny, 527 F.2d 479, 482 (9th Cir. 1975) (categorizing "phreakers" as illegal users of a telephone line). *See also* Michael Lee et al, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 857 (1999) (citing Senate testimony that describes "phreaking" as the use of telephone systems to make fraudulent phone calls or the manipulation of the telephone system).

[83] Some studies indicate that electronic communications have caused the amount of child pornography to skyrocket 1,500% since the late 1980s, and there are fears that increased wireless connections will continue this unfortunate trend. *See* David Barett, *Mobile Phones Linked to Internet May Fuel Rise in Child Porn Offences*, INDEPENDENT (UK), Jan. 12, 2004, *available at* http://news.independent.co.uk/uk/crime/story.jsp?story=480353. The widespread availability of information helps dishonest people find secret locations where criminal data is stored. *See id.*; *Child Porn Crime Rockets,* JOURNAL (U.K.), Jan. 12, 2004, at 11; Kerr, *supra* note 33, at 1603: "Two decades ago, a pedophile seeking to obtain illegal images of child pornography would seek out a book or magazine containing the images. Today, the same pedophile likely would turn to the Internet, and seek out chat rooms and underground clubs that distribute these illegal images in digital form."

[84] The FBI has stated that up to 80% of all hackers' connections are made through specialized connections to computers that are not connected to the Internet. *See* CYBERWARS: ESPIONAGE ON THE INTERNET 114-15 (Jean Guisnel ed., 1999).

[85] *See* Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, at para. 20 (1992), *available at* http://www.mit.edu/hacker/hacker.html (last visited Dec. 15, 2003).

[86] *Id.* at para. 21.

the criminal code up to date with computer/telephone interface (*i.e.,* modem) technology.[87]

¶ 28 Before the telephone system became highly digitized, it was open to attack by certain homemade analog devices used to trick the system and make free phone calls. Courts have convicted people for the following types of phreaking: (1) the use of "red boxes,"[88] which enable people to make free phone calls from payphones;[89] (2) the use of "blue boxes,"[90] which allow people to make phone calls from any phone by emitting a sound over a frequency that leads the computer to believe the phone call was made by an operator;[91] (3) the use of "black boxes,"[92] which send false voltage signals when a caller picks up a call so that the calling party is not charged;[93] and (4) the use of "silver boxes," which create special tones that only operators use (*e.g.*, tones that can be used to take control of certain PBX[94] systems and connecting calls).[95] The use of these devices is certainly criminal, since the devices are used to bypass the per-minute charge that the telephone company imposes for making a phone call. In fact, the government has had little trouble prosecuting these activities under the Wire Fraud Act,[96] particularly in the 1970s (although massive reform of the Act was necessary to keep up with modern computer crimes).[97]

[87] 18 U.S.C. § 1030 (2004) is the basic federal computer crime provision. *See* discussion *infra* Section IV. Originally, it was known as the Counterfeit Access Device and Computer Fraud and Abuse Act, and it was amended several times. Pub. L. No. 98-473, § 2102(a), 98 Stat. 1837, 2190 (1984); Computer Fraud and Abuse Act, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986); Pub. L. No. 100-690, § 7065, 102 Stat. 4404 (1988); Pub. L. No. 101-73, § 962(a)(5), 103 Stat. 502 (1989); Pub. L. No. 101-647, § 1205(e), § 2597 (j), § 3533, 104 Stat. 4831, 4910, 4925 (1990); Pub. L. No. 103-322, § 290001 (b)-(f), 108 Stat. 2097-2099 (1994); Pub. L. No. 104-294, § 201, 110 Stat. 3488, 3491-94 (1996). The original act and the 1986-1996 amendments were all codified as 18 U.S.C. § 1030, which was then amended by the Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[88] The hacking website http://hackfaq.org contains a detailed listing of how-to instructions for various types of devices. The Red Box FAQ can be found at http://www.hackfaq.org/telephony-01.shtml (last visited Jan. 10, 2004). Devices are also still available on the market to detect and counter such products. *See* http://www.tekind.com/telecommunications/antifraud.htm (last visited Jan. 10, 2004) (advertising a product used to prevent fraudulent coin calls attempted by red boxes).

[89] *See, e.g.,* State v. Conaway, 319 N.W.2d 35, 38-39 (Minn. 1982) (noting the seizure and prosecution of a defendant for the possession of red boxes used for telephone fraud).

[90] For a description of the functionality of a blue box, see http://www.hackfaq.org/telephony-06.shtml (last visited Jan. 10, 2004).

[91] *See, e.g.,* United States v. Disla, 805 F.2d 1340, 1344 (9th Cir. 1986) (prosecution under 18 U.S.C. § 1343 for fraudulent use of a blue box).

[92] For a description of the functionality of a black box, see http://www.hackfaq.org/telephony-08.shtml (last visited Jan. 10, 2004).

[93] *See, e.g.,* United States v. Harvey, 540 F.2d 1345, 1348-50 (8th Cir. 1976) (regarding criminal procedure matters in the prosecution of a defendant who possessed both a black box and a blue box).

[94] A PBX is a "Private Branch Exchange," and it is a private telephone network used within an enterprise. It can connect to the regular telephone network as well.

[95] For a description of the functionality of a silver box, see http://www.hackfaq.org/telephony-36.shtml (last visited Jan. 10, 2004).

[96] Wire Fraud Act, 18 U.S.C. § 1343 (2004).

[97] As Judge Heartfield observed, the mail and wire-fraud statutes were often incapable of combating computer crime that did not involve interstate commerce. Thus, Congress enacted 18 U.S.C. § 1030 and amended it in 1986, 1988, 1989, 1990, 1994, and 1996. Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d 926, 930 n.6 (E.D. Tex. 1999).

¶ 29 Phreaking crimes have evolved over time. As networks became more computerized in the late 1980s, "hacking" and "phreaking" merged to create a new hybrid form of telephone fraud and computer crime. In turn, telephone companies became much more successful at identifying and prosecuting telephone fraud as it evolved from hijacking the system with analog "blue boxes" and similar devices to using computerized access codes. Convictions for the use of homemade phreaking boxes appear to be less frequent today, since the telephone companies have migrated to modern computerized switches and controls.

¶ 30 Telephone network operators had strong incentives to modernize. In 1981, the AT&T phone system was "phreaked" by Ian Murphy (also known as "Captain Zap"), who changed the phone system's internal clocks so that everyone who made calls during the day was charged the nighttime rate. This stunt earned Murphy the first conviction for hacking,[98] a permanent place in the hacker's hall of fame,[99] and a job as a hacking security consultant.[100] And, of course, a major Hollywood hacking movie called *Sneakers* was based on Murphy's feat.[101]

¶ 31 Phreaking and hacking terms have also merged. For example, network specialists who want to stop "attackers" must use secure "firewalls."[102] These firewalls must be strong enough to identify and resist all types of attackers, even those using "Trojan horse" techniques[103] as a means of delivering their arsenal. Network "truces" must be declared in order to facilitate certain file sharing (*e.g.*, by configuring certain computers

[98] Mark Goodman, *Hacker for Hire*, PEOPLE, Oct. 19, 1992, at 151 (noting that Murphy was the first hacker to be convicted and that he was let off with community service and served very little jail time).

[99] *See* Delio, *supra* note 36. *See also Outlaws & Angels Hall of Fame: Ian Murphy* (TLC/Discovery Channel broadcast) *available at* http://tlc.discovery.com/convergence/hackers/bio/bio_14.html (last visited Jan. 14, 2004); Michael Fitzgerald, *Nine Famous Hacks*, EXTREMETECH, Jan. 8, 2004, *available at* http://story.news.yahoo.com/news?tmpl=story&u=/ttzd/20040108/tc_techtues_zd/115859&cid=1739&ncid=1729 (Murphy is awarded the number one position in this recent article).

[100] Murphy is the founder of the company IAM/Secure Data Systems, Inc. *See* Goodman, *supra* note 98 (stating that in 1992, when the article was written, Murphy was making more than $250,000 per year); *"Captain Zap" Announces New Internet Security Initiative,* BUS. WIRE, Sept 18, 2000, *available at* http://www.findarticles.com/cf_dls/m0EIN/2000_Sept_18/65276536/p1/article.jhtml. *See also* Erik Sandberg-Diment, *The Executive Computer*, N.Y TIMES, July 28, 1985, at 13. Arrested in 1981 and later convicted on felony charges, Captain Zap, a self-proclaimed "penetration and countersurveillance expert," could not make an honest living in the computer security industry until after he was convicted of stealing close to half a million dollars' worth of computer products. *Id.*

[101] SNEAKERS (Universal Studios 1992). *See* Internet Movie Database, *available at* http://www.imdb.com/title/tt0105435/ (last visited Jan. 12, 2004). *See also Outlaws & Angels Hall of Fame: Ian Murphy* (TLC/Discovery Channel broadcast) *available at* http://tlc.discovery.com/convergence/hackers/bio/bio_14.html (last visited Jan. 14, 2004); (awarding Murphy "Discovery Channel Hall of Fame" status and noting that he is the character basis for the movie *Sneakers*).

[102] A "firewall" is a combination of hardware and software used to limit the vulnerability of computers to outside attacks. See NEWTON, *supra* note 11, at 299-300.

[103] A "Trojan horse" is the generic term for a malicious program that causes damage but that is disguised as something benign. The term originally comes from Greek mythology, where Greek soldiers hid inside a hollow wooden horse and thus were transported into the city of Troy; as a result of their deception, the Greeks were able to conquer the Trojans. A "Trojan horse program" is a computer program with an apparently (or legitimately) useful function that contains additional hidden aspects that can cause damage and allow an unauthorized user to gain access to the target computer's files and functionality. *See* DAVID ICOVE ET. AL., COMPUTER CRIME: A CRIMEFIGHTER 'S HANDBOOK 427 (1995).

as "de-militarized zones").[104] Although not all terms can be traced to the movie *WarGames,* warfare terminology has certainly become deeply entrenched in activities such as hacking, phreaking, and cracking.

¶ 32 The popular hacking magazine *Phrack* takes its name from a hybrid term inspired by the merger of *phr*eaking and h*ack*ing. One of the more infamous cases involving phreaking and hacking was the *Coconut Connection* case, where a Hawaiian company sold hacked calling cards to legitimate businesses. The case was novel because it involved several computer systems that accessed up-to-the-minute information on calling cards and distributed that information to companies (who thought they were legitimate) before the telephone company could identify them as stolen.[105] *Forbes* called the *Coconut Connection* case one of the largest telecommunications fraud cases on record. In fact, the case involved twenty arrests, seizure of twelve computer systems, and $125 million in fraud losses annually.[106]

¶ 33 Both the Murphy and *Coconut Connection* cases involved phreaking and both were unmistakably criminal matters. Not all cases are so clear. Computer crime and computer security are considered criminal activities by some, but are considered games by others. Distinguishing between the two is not always easy. However, in general, hackers identify problems in a network, and phreakers exploit vulnerabilities in telephone networks to make phree phone calls. The Internet has complicated the situation by enhancing the ability to share information exponentially, and as a consequence, the gray area that existed between "good" hackers on the one hand and "bad" hackers (*e.g.*, phreakers) on the other has blurred even more.

IV. WARDRIVING AND WARCHALKING

¶ 34 Wireless networking has created a new shade of gray between hacking and phreaking. Wireless networking, in fact, is a standards-setting success story. Unlike many of the new technology products of the 1990s, many of which pitted consumers against manufacturers in "standards wars" (as happened with 56k modems,[107] DVDs,[108]

[104] At the end of World War II, a demilitarized zone was set up between North and South Vietnam. Now, however, DMZ often refers to neutral computer zones that are set up between two systems that are "untrusted" (*i.e.,* the systems are not certified as secure). *See* NEWTON, *supra* note 11, at 234.

[105] *See* William G. Flanagan & Brigid McMenamin, *For Whom the Bells Toll,* FORBES, August 3, 1992, at 60 (describing the details of the *Coconut Connection* case).

[106] *Id.*

[107] Two conflicting 56k modem protocols—one created by Rockwell and another created by 3Com—kept many users from upgrading from 28k modems to 56k modems. Ultimately, the matter was mediated by the International Telecommunications Union, and the sides reached an agreement on a single standard at the end of 1997. *See* Frederick Rose, *Modem Makers Reach Accord on Standards*, WALL ST. J., Dec. 8, 1997, at B6.

[108] Two rival technologies for the high-definition home video market kept consumers from fully embracing any product for years for fear that their devices would not be compatible with the final de facto standard. In 1997 and 1998, DVD and DIVX standards were being sold through different distribution channels. Most consumers waited until DVD was declared the clear winner in the battle before purchasing a system. *See* Evan Ramstad, *As Prices Tumble, Sales of DVD Players Explode for the Holidays*, WALL ST. J., Dec. 9, 1999, at B1 (describing the standards war between DVD and DIVX).

wireless telephony,[109] and HDTV[110]), the Wi-Fi wireless networking standard quickly received widespread consumer acceptance as a *de facto* standard. In the mid 1990s, the Institute of Electrical and Electronics Engineers (IEEE) created a working group to promote a universal wireless networking standard.[111] By 1997, the working group had agreed on the 802.11 standard, which specified various protocols and a frequency of 2.4 GHz. In 1999, the IEEE accepted and published the 802.11b amendment, which dramatically increased the potential data rate to 11 Mbps. This data rate is widely viewed as a key component in the rapidly-expanding consumer networking market.[112] With the recipe complete, manufacturers began selling 802.11b products the very same year. At that time, a Wireless Access Point (WAP) cost more than $1,000.[113] In 2000, however, Apple introduced its far less expensive AirPort product, thus creating pressure to dramatically reduce component prices.[114] Acknowledging that consumers rarely embrace technical terms, an industry group called the Wireless Ethernet Compatibility Alliance (WECA) created a logo and a common name, Wi-Fi, short for "Wireless Fidelity."[115] Today, a Wi-Fi WAP can be had for as little as $50. Wireless access cards are available for notebooks for around $20, and often are already built-in, not unlike modem ports or Ethernet ports.[116] Sales of Wi-Fi products have been one of the great technology success stories of the past decade.[117]

¶ 35 Wi-Fi created new opportunities for many different sectors. Consumers purchased the product to set up wireless access for their homes and small businesses, and companies like Starbucks embraced the idea in order to encourage users with laptops to patronize their coffee shops.[118] Service providers also began marketing Wi-Fi services to travelers

[109] There are multiple digital standards for wireless telephony, including TDMA, GSM, different variations of CDMA, and many others. Each wireless standard is incompatible with the other, and consumers must purchase multimode phones to use the service of providers that send signals based on a different standard. *See* Stephanie N. Mehta, *The Search Continues for a Single Wireless Standard*, WALL ST. J., Nov. 18, 1999, at B8 (describing the different standards and the emergence of multimode phones).

[110] Standards are finally emerging now for HDTV; however, for many years an intercontinental battle raged between Europe, the United States, and Japan. *See* Bob Davis, *Europe Defeats Japan's Proposal on TV Standard*, WALL ST. J., May 25, 1990, at B4 (describing the different standards proposals in Europe, the United States, and Japan and outlining the different positions of the players).

[111] The Institute of Electrical and Electronics Engineers, Inc. (IEEE) is a non-profit technical professional association that promotes standards in many technical fields. IEEE 802 Working Group documents and information about the history of the Wi-Fi standard-setting process can be accessed on a special IEEE website, *available at* http://www.ieee802.org (last visited Jan. 15, 2004).

[112] DUNTEMANN, *supra* note 6, at 372.

[113] *Id.* at 8.

[114] *Id.* at 10.

[115] In 2002, the Wireless Ethernet Compatibility Alliance changed its name to the Wi-Fi Alliance. *See* http://www.wi-fi.com (last visited Jan. 15, 2004).

[116] *See* Nick Wingfield, *Anytime, Anywhere: The Number of Wi-Fi Hot Spots is Set to Explode*, WALL ST. J., Mar. 31, 2003, at R6 (noting that by 2005, 91% of computers will come standard with Wi-Fi capabilities and that the product price for all components has dropped to a commodity level).

[117] *Id.*

[118] As of mid-2003, more than 2,000 Starbucks coffee shops had Wi-Fi installed, and around 25,000 people had accessed the Internet from Starbucks shops each week. *See Bubble Trouble*, ECONOMIST, June 28, 2003 (describing the massive Wi-Fi deployment craze in 2002-2003).

and others at hotels and airports.[119] The rapid introduction of wireless access also attracted hackers, who, in the spirit of *WarGames* (and with an entrenched legacy of wardialing), invented two new activities called wardriving and warchalking. As it turns out, many of the wardialers who were not prosecuted for their criminal intent actually had performed a useful public service by spurring improvements in modem security. The next generation of war gamers then turned to the vulnerabilities within new Wi-Fi technologies. The *WarGames* terminology survived, and it mutated. In addition to the *WarGames* and wardriving legacy, "War" also took on a new meaning: Wireless Access Reconnaissance.[120]

¶ 36 Wi-Fi has the same basic core problem that many computer networks had during the wardialing days: the default configurations of many commercial devices leave them open to all users.[121] Thus, an individual who installs a wireless network as a "plug-and-play" product[122] generally installs an *open* network, where virtually any user within the range of the device may access the Internet. Although it is fairly easy to "close" (*i.e.* secure) Wi-Fi networks via built-in encryption software that is resident on nearly all systems, many users simply fail to activate the software.[123]

¶ 37 Wardrivers are primarily interested in open networks. Although it is not impossible to crack the security of closed wireless networks,[124] more than half of the world's wireless networks are open and unlocked, leaving plenty of "low hanging fruit" ripe for the picking.[125]

[119] Many of these installations are done by various providers, and multiple subscriptions are often required. *Id.*

[120] *See* DUNTEMANN, *supra* note 6, at 369.

[121] Many devices come with default modes that are "open," which creates (sometimes unknown) vulnerabilities for users. The Carnegie Mellon Software Engineering Institute regularly researches and publishes known problems, called Vulnerability Notes. *See, e.g.*, Jason Rafail, *Vulnerability Note VU#557136: Cayman Gateways Ship with Null Administrative and User Level Passwords*, CERT/Coordination Center, *available at* http://www.kb.cert.org/vuls/id/557136 (last visited Jan. 1, 2004). *See also* DUNTEMANN, *supra* note 6, at 279.

[122] In the early 1990s, it was clear that devices requiring little configuration would not only sell better, but that they would also reduce customer service costs. Therefore, connections between different devices became simpler, and default configurations allowed users to plug devices together and use them ("plug and play") became the fashion. Apple, maker of the Apple Macintosh computer, is credited as one of the innovators of this concept. *See* Walter S. Mossberg, *One Task PCs Fail to Simplify: Adding Gadgets to Your PC*, WALL ST. J., Mar. 26, 1992, at B1 (describing the problem of adding additional hardware to PCs and crediting the Apple Macintosh—in 1992, when the article was written—with being "as close as you can come today to a mass-market 'plug-and-play' computer").

[123] *See A Network of Drive-By Spies,* FIN. POST CAN., Aug. 5, 2003, *available at* http://www.digitaldefence.ca/html/article_35.shtml (citing a Toronto wireless security specialist who believes that sixty to seventy percent of all existing wireless networks have not set up any security at all).

[124] See Nick Wingfield, *The Best Way to Protect Your Wi-Fi Connection*, WALL ST. J., Sep. 15, 2003, at R12, for an excellent overview of WEP security measures, their evolution, and ongoing security problems, as well as tips on making networks more secure.

[125] In 2001, reports indicated that as many as 90% of wireless networks had no security. The situation has improved, but most believe a large number of networks are still open. *See* Xeni Jardin, *Wireless Hunters on the Prowl,* WIRED, July 2, 2003, *available at* http://www.wired.com/news/wireless/0,1382,59460,00.html.

¶ 38 In the following sections, the historical, ethical, and legal aspects of wardriving and warchalking will be reviewed. Furthermore, we will explore the significance of relevant laws and related writings, including a critical FBI memorandum, the Computer Fraud and Abuse Act, and the Electronic Communications Privacy Act. Finally, we will analyze the details of prosecutions for wardriving-related acts and review proposed state legislation.

A. Wardriving

¶ 39 We will begin our discussion by describing the act of wardriving in greater detail. The practice of wardriving is similar to using a scanner for radio.[126] Wardrivers often connect a GPS device to their Wi-Fi-enabled laptop to find the exact location of the networks that they scan. Wardriving software is freely available on the Internet, notably NetStumbler[127] for Windows, MacStumbler[128] for Macintosh, and Kismet[129] for Linux. There are even specialized miniature devices that do nothing other than detect the presence of Wi-Fi networks.[130] For better range, wardrivers can connect specialized antennas, such as the cylindrical canisters in which Pringles brand potato chips are sold, to their notebooks.[131] Pioneer wardriver Peter Shipley claims that he is able to use homemade specialized antennas to make connections to open networks from as far away as twenty-five miles.[132]

[126] Scanning in most frequencies is a legal and protected right so long as users do not violate the Electronic Communications Privacy Act, 18 U.S.C. § 2511 (2004), discussed *infra* at Section IV.E. Initial industry claims indicated that spread spectrum technology made it impossible to scan, but since 802.11 became the standard, this claim proved false because anyone with a Wi-Fi card could become a scanner. *See* Matthew Gast, *Wireless LAN Security: A Short History*, O'REILLY WIRELESS DEVCENTER, Apr. 14, 2002, *available at* http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html. The author explains:

> Vendors first claimed that spread-spectrum modulation made it hard to build a receiver. That assertion was true in a limited sense. Traditional RF receivers listen at a narrow band for the signal, and spread spectrum uses wide bands. However, the claim is also a silly assertion because the receiver of a frame must, by definition, be able to receive and process it. Therefore, any 802.11 interface must, by definition, be the receiver that vendors claimed didn't exist. *Id.*

[127] *See* http://www.netstumbler.com (last visited Jan. 18, 2004).

[128] *See* http://www.macstumbler.com (last visited Jan. 18, 2004).

[129] *See* http://www.wirelesscon.com (last visited Jan. 18, 2004).

[130] *See* Walter S. Mossberg, *The Mossberg Solution: Tracking the Elusive Hot Spot*, WALL ST. J., Nov. 5, 2003, at D4 (describing a device the size of a credit card called the "Kensington Wi-Fi Finder" that sells for $29.99 and that does nothing but detect the presence of Wi-Fi spots).

[131] Even sophisticated agencies, such as the federal government, use Pringles cans to improve reception. "A Pringles can is ideal because of its shape -- a long tube that lets someone point it at specific buildings -- and its aluminum inner lining. It acts like a satellite dish, collecting signals and bouncing them to the receiver, which is then wired into a laptop." D. Ian Hopper, *Agency Probes D.C. Wireless Network*, AP ONLINE, Sept. 30, 2002, *available at* http://www.govtech.ne/news/oldnews.phtml.

[132] Many different antennas on the market increase the range of Wi-Fi computers. These antennas can be made at home or purchased in stores, and they can increase the Wi-Fi computer range by several street blocks to several miles. *See* Peter Shipley, *Open WLANs, the Early Results of WarDriving*, *available at* http://www.dis.org/filez/openlans.pdf (last visited Dec. 14, 2003) (showing photographs of antennas and claiming 25 miles of access); Sandra Kay Miller, *War Driving*, INFO. SECURITY MAG., Nov. 2001,

¶ 40 Wardriving is not just an occasional activity. In a study conducted by the computer security division of KPMG, a dummy access point was set up to observe the activity of wardrivers.[133] The study found that, on average, there were 3.4 attempts to access its dummy wireless network per day.[134]

¶ 41 Wardriving has been highly publicized, particularly through large-scale security firm-promoted "worldwide wardrives."[135] The media coverage has been impressive and cannot be overstated. Feature articles on wardriving (and on warchalking) have appeared in several publications in the United States,[136] the United Kingdom,[137] Germany,[138] Belgium,[139] Canada,[140] Australia,[141] and elsewhere.[142] Hundreds of security articles have been written on the topic. The question remains: Why wardrive? Free wireless access may be one motivation.[143] Most wardrivers vehemently assert that they are proving a point. As Peter Shipley notes: "People don't believe there's a security problem if you don't prove it to them."[144] There are undoubtedly some benevolent wireless "neighborhood watchmen" who hope to better the world and make it safer by revealing security holes. More likely, however, is that wardrivers fall under one or more of the following categories: (1) they innocently wish to gain free wireless access in their neighborhoods, perhaps at a local coffee shop; (2) they have commercial motivations and

available at http://infosecuritymag.techtarget.com/articles/november01/technology_wardriving.shtml (describing the different products used in wardriving, including antenna accessories to increase range).

[133] *Commuters Hack Wireless Networks*, BBC NEWS, Mar. 26, 2003, *available at* http://news.bbc.co.uk/1/hi/technology/2885339.stm.

[134] *Id.*

[135] *See* Bulkeley, *supra* note 32 (describing wardriving and warchalking).

[136] *See e.g.*, *id.*; Christine Tatum, *War Chalking Erases Limits of Wireless Clusters*, CHI. TRIB., AUG. 26, 2002, at 3; Dominique Deckmyn, *War Chalking Is Illegal*, ZDNET.BE, Oct. 2, 2002, *available at* http://www.zdnet.be/print.cfm?id=21336 (article in Belgian; noting that the practice seems to be widespread in Athens, Georgia and San Jose, but has not yet reached Chicago); Tony Bridges, *Laptops Provide Security Leaks*, TALLAHASSEE DEMOCRAT, Nov. 23, 2003, *available at* http://www.tallahassee.com/mld/democrat/7329089.htm (describing the activities of a wardriver who accessed the ports and other areas of computers in a college sorority house); Jeff Smith, *The Drive to Connect: Chalk, Software Sniff out Vulnerable Wireless Networks*, ROCKY MOUNTAIN NEWS, July 21, 2003, at 1B (describing the work of a warchalker in Denver).

[137] *See, e.g.*, Mark Ward, *Write Here, Right Now*, BBC NEWS ONLINE, July 1, 2002, *available at* http://news.bbc.co.uk/1/hi/in_depth/sci_tech/2000/dot_life/2070176.stm; Colin Barker, *We Have Nothing to Fear but Fear Itself*, COMPUTING, Sept. 27, 2002, *available at* http://www.computing.co.uk/Features/1135465 (describing warchalking activity in London).

[138] *See, e.g.*, Andreas Eichelsdörfer & Thomas Fischer, *Signs - Zeichen*, PC BUSINESS, February 2003, *available at* http://www.pcbusiness-online.de/magazin/pcb0203/editorial.shtml; *Neuer illegaler Trend: Warchalking*, PC WELT.DE, July 7, 2002, *at* http://www.pcwelt.de/news/internet/24985/.

[139] *See, e.g.*, Deckmyn, *supra* note 136.

[140] *See, e.g.*, Tyler Hamilton, *Insecure Wireless Networks Exposed*, TORONTO STAR, Sept. 10, 2002, at C1.

[141] *See, e.g.*, Jeanne-Vida Douglas, *Wireless Hacking: The Art of Wardriving*, ZDNET AUSTL., June 5, 2002, *available at* http://www.zdnet.com.au/news/security/ 0,2000061744,20265777,00.htm.

[142] *See* Graeme Wearden, *Wardriving Sparks Wireless Treasure Hunt*, ZDNET UK, Nov. 14, 2003, *available at* http://news.zdnet.co.uk/communications/wireless/0,39020348,39117912,00.htm (describing a massive wardriving event scheduled for December 7, 2003, in New Zealand).

[143] *See* Wingfield, *supra* note 16.

[144] Kevin Poulsen, *War Driving by the Bay*, SECURITYFOCUS, Apr. 12, 2001, *available at* http://www.securityfocus.com/news/192 (quoting wardriving "inventor" Peter Shipley).

hope to sell security services; or (3) they have dishonest motives and hope to surreptitiously access networks information, send anonymous spam, or acquire illegal data. A discussion of the motivations and ethics of these groups is addressed below in Section VII.

B. Warchalking

¶ 42 From wardriving, the discussion logically shifts to an analysis of warchalking. The practice of "chalking" originates from the marks that homeless persons made during the Great Depression to signal a friendly house.[145] Warchalkers use chalk marks to denote the status of wireless nodes. For example, a chalk mark of the symbol ") (" denotes an open network, while a chalk-marked "O" denotes a closed network. A popular website has been created to standardize the warchalking symbols used.[146] Ironically, warchalking does not necessarily denote a "friendly" house; in fact, the practice makes no statement whatsoever regarding the "friendly" disposition of network owners. Network owners may not even be aware that others are using their WAP. Like wardriving, warchalking has received a great deal of media attention, but some commentators (most reputably, those who have published articles in *The Economist*) believe that the practice itself is quite rare.[147]

¶ 43 In practice, many websites publish maps of WAPs in major cities, virtually "chalking" the existence of open nodes on the Internet.[148] Although such publications may serve a useful security purpose by *indirectly* notifying network users of vulnerabilities (assuming those users are aware of these sites), this form of Internet publication also leaves unwitting WAP owners open to possible invasions of privacy. This serious ethical problem illustrates an important distinction in the debate: not all wardrivers are warchalkers. In fact, many wardrivers do not share the open network data they find, or, in some cases, they may contact WAP owners, inform them of the vulnerability, and perhaps attempt to sell them security services. In contrast, warchalkers do not always display the same ethical values exhibited by wardrivers. Returning to the neighborhood watchmen analogy, chalking the location of an open node (either on the side of a building or on the Internet) without notifying the owner is akin to chalking a sign near a home that states "*this door is unlocked; there is no security here*." Given the additional risk this poses to the home (or WAP), it is unlikely that the owner would agree to such a posting.

[145] *See* Smith, *supra* note 136. *See also* http://www.slackaction.com/signroll.htm (last visited Dec. 15, 2003) (noting the symbols that hobos used to communicate with chalk marks).

[146] *See* http://www.warchalking.org/ (last visited Dec. 15, 2003). The warchalking signs are consistent throughout the web and in print literature. *See e.g.,* DUNTEMANN, DRIVE-BY WI-FI GUIDE, *supra* at note 6, at 372.

[147] *See The Revenge of Geography*, ECONOMIST, Mar. 15, 2003, at 22 (describing warchalking and noting that it "has gained much attention in the media, however, hardly anybody actually does it").

[148] *See* DUNTEMANN, *supra* note 6, at 372 (describing warchalking). For a sample Internet-based warchalking map, see http://www.worldwidewardrive.org (last visited Jan. 16, 2004).

C. The FBI Memorandum

¶ 44 Predictably, wardrivers assert that their actions are legal.[149] Wardriving literature advises wardrivers what to do in the event that they are stopped by a police officer. Such stops apparently happen with some frequency, since wardrivers tend to drive slowly, swerve, and look frequently at their laptops.[150] To date, there are no published cases that squarely address the topic. However, this lack of concrete data has not dissuaded government officials from issuing memoranda and trying cases that are (at least tangentially) related to wardriving. In 2002, for example, the FBI issued an unofficial[151] (but highly publicized)[152] memorandum suggesting that some elements of wardriving may not be illegal (e.g., the mere identification of sites), while at the same time providing a warning about collateral activities:

> *Identifying* the presence of a wireless network may not be a criminal violation, however, there may be criminal violations *if the network is actually accessed* including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations.[153]

¶ 45 The FBI memorandum is not law. However, when wardriving-related cases are tried (and it is likely that such cases will arise), an understanding of the government's position will be critical. It will be important to review and understand the government's position, the statutes that have been passed, and the relevant case law regarding matters of computer access.[154] Moreover, the FBI memorandum departs somewhat from FCC Chairman Powell's "guiding principles for the industry," which encourage users to attach (presumably open-access) devices to their networks.[155] Finally, by stating that "identifying the presence of a wireless network may not be a criminal violation," the FBI memorandum completely ignores the ethical dilemmas related to warchalking.

[149] *See* http://web.archive.org/web/20030618120137/http://www.wardrivingisnotacrime.com/index.html (last visited Dec. 15, 2003) (archival, original site is defunct).

[150] *See* Audit, *How Not to Get Pulled Over by LEOs (Law Enforcement Officers) v0.4*, Feb. 19, 2004, *available at* http://www.michiganwireless.org/staff/audit/wardriving/.

[151] Memorandum from Bill Shore, FBI Agent, Wireless Networks: Warchalking/Wardriving, *available at* http://www.politechbot.com/p-03884.html (July 8, 2002). It has been reported that the FBI agent claimed that his memo was not an official communication but instead was "just a release I made to the Pittsburgh infraGard Chapter . . . it is not really an FBI warning, advisory . . . I just thought it would be relevant and interesting to our local chapter." *See* Posting of Declan McCullaugh, declan@well.com, to politech@politechbot.com, *FBI Releases Advisory About 802.11-Spotting "Wardriving,"* Aug. 13, 2002, *at* http://www.politechbot.com/p-03888.html.

[152] *See* Levy, *supra* note 10 (discussing the impact of the memorandum); Dan Verton, *New Risk for Wireless Access Points*, COMPUTERWORLD, Aug. 19, 2002, at 1 (discussing the FBI memo and describing it as follows: "Federal law enforcement officials are warning companies of a systematic effort by computer enthusiasts and possibly hackers to mark and map nonsecured Wi-Fi 802.llb wireless access points in many major metropolitan areas").

[153] Shore, *supra* note 151 (emphasis added). *See also* Rob Flickenger, *The FBI Takes an Interest in War Chalking and War Driving*, O'REILLY DEVELOPER WEBLOGS, Aug. 13, 2002, *available at* http://www.oreillynet.com/pub/wlg/1827 (discussing and providing links to the FBI memorandum).

[154] *See* Kerr, *supra* note 33, at 1624, 1631, 1641 (a comprehensive review of the problems of the interpretation of "authorization" and "access" in computer crimes).

[155] See Powell, *supra* note 21, at 5.

Regardless of its legality, the act of warchalking balances on a fine ethical line.

D. The Computer Fraud and Abuse Act

¶ 46 While the FBI memorandum may not carry legal weight, the Computer Fraud and Abuse Act (CFAA) may apply, directly or indirectly, to wireless network access. The CFAA was passed in 1984, before wireless access was a reality. Thus far, there are no reported cases under the CFAA related to wireless access. A strict textual interpretation of the Act indicates that its purpose is to create a cause of action for intentionally accessing *protected* open systems. The CFAA is enforceable against whoever "*intentionally* accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any *protected* computer if the conduct involved an interstate or foreign communication."[156] The CFAA also provides for the punishment of whoever "intentionally accesses a protected computer without authorization and, as a result of such conduct, recklessly causes damage."[157] Cases tend to focus on (1) intent,[158] (2) whether or not the computer system and data are protected,[159] and (3) the impact of user agreements on future claims.[160] Most of these elements would also be applicable in a wireless context.

¶ 47 However, there are additional considerations. For example, contractual conditions may exist between the individual who installs the WAPs and her Internet Service Provider (ISP). Thus, the owner of the WAP may be held liable if she offers it as an open node for use by others.[161] Indeed, one ISP sent out its own wardrivers to verify that its subscribers are not violating their user agreements.[162] Although such acts would typically fall under breach of contract, they could also trigger CFAA liability for both the user and the WAP owner, even if a direct contract or click-through agreement does not exist between the user and the WAP owner. Courts have imposed liability under the CFAA in similar situations. In one case, a user sent spam in violation of the ISP's terms of service.[163] Another court granted an injunction where an individual used a false Hotmail account to send spam. Hotmail Corporation was allowed to show "damage" in the form of the computing power diverted by Hotmail's servers to handle the spam

[156] 18 U.S.C. § 1030(a)(2)(B) - (C) (2004) (emphasis added).

[157] 18 U.S.C. § 1030(a)(5)(iii).

[158] *See e.g.,* United States v. Sablan, 92 F.3d 865, 867-68, 869 (9th Cir. 1996) (holding that the government is not required to prove that the defendant intentionally damaged computer files, but only that the defendant intentionally *accessed* the computer without authorization.)

[159] *See, e.g.,* Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1325-26 (S.D. Fla. 2003) (a civil CFAA case holding that the plaintiff's computer system was protected and that the protected information included customer lists and other trade secrets).

[160] *See, e.g., In re* America Online, Inc., 168 F. Supp. 2d 1359, 1369-71 (S.D. Fla. 2001) (discussing the scope of "exceeds authorized access" under the CFAA).

[161] *See, e.g.,* America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (imposing liability under the CFAA for sending spam in violation of the users' terms of service).

[162] *See* Langley, *supra* note 18 (reporting that AT&T Broadband sent wardrivers to find customers in breach of contract).

[163] *See In re America Online*, 46 F. Supp. 2d at 448.

communications and the multitude of consumer replies to the false addresses.[164] In accordance with this line of jurisprudence, a court could find damages when a wardriver causes excess computing resources to be used by the network owner or ISP by accessing a WAP to download files.

¶ 48 Notably, the first version of the CFAA was passed shortly after the release of *WarGames*, almost as if the law were drafted to directly address the types of activities carried out by Lightman. Initially designed to protect classified information on *government* computers and "federal interest computers,"[165] the CFAA was amended in 1986 to "provide additional penalties for fraud and related activities in connection with access devices and computers."[166] The scope of the CFAA has since been increased through various amendments to cover all kinds of computer access.[167]

E. The Electronic Communications Privacy Act

¶ 49 The Electronic Communications Privacy Act (ECPA), also known as the "Wire Tap Law," may also apply to wardriving since wardriving is a form of wireless scanning. The ECPA holds that:

> [It shall not be unlawful] for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.[168]

¶ 50 The ECPA also imposes federal penalties on anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[169] In short, the ECPA is an anti-eavesdropping law. Violations of the ECPA have five essential elements. An individual must (1) intentionally (2) intercept, endeavor to intercept, or procure another person to intercept (3) the contents of (4) an electronic communication (5) using a device. The law has been used to target various acts of wireless interception and signal theft.[170]

[164] *See* Hotmail Corp. v. Van Money Pie Inc., 1998 U.S. Dist. LEXIS 10729, at *5 (N.D. Cal. 1998).

[165] *See In re America Online*, 168 F. Supp. 2d at 1374 (discussing the legislative history, noting that the CFAA has expanded beyond federal and financial systems, and quoting the Senate Report:

> As computers continue to proliferate in business *and homes*, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary framework to fight computer crime (emphasis added in original)).

[166] *Id.*

[167] *See* N. Tex. Preventative Imaging, L.L.C. v. Eisenberg, 1996 WL 1359212, at *4-6 (C.D. Cal. 1996) (discussing legislative history of the CFAA).

[168] 18 U.S.C. § 2511(2)(g)(v) (2004).

[169] 18 U.S.C. § 2511(1)(a).

[170] United States v. Davis, 978 F.2d 415, 419-20 (8th Cir. 1992) (holding it unlawful to intentionally intercept commercial satellite programming, particularly where the transmissions are

¶ 51 Cases of interception and signal theft, however, have little bearing on the act of wardriving itself, although they may be relevant to derivative acts. If a wardriver truly does nothing more than identify open networks, then she is only checking the technical availability of a network, not intercepting the communications of others. Although the technical verification process involves a computer response to the wardriver's request, this response is provided by open and automated computer protocols. The privacy of the WAP owner's communications is not compromised at any point. Like burglary and criminal trespass, privacy laws are only likely to apply to specific intent crimes (*e.g.*, breaking and entering someone else's WAP with the intent to eavesdrop therein).[171]

F. Prosecution of Wardriving-Related Acts

¶ 52 As with any new and untested area of law lacking published cases, it is helpful to review the basis for application of relevant statutes (as done above), as well as review trends in prosecutions and indictments. Of course, such cases have no legal relevance *per se*, since they do not have any *stare decisis* character. Nevertheless, such data can highlight the contemporary problems confronting the government and the private sector. Each of the three cases that will be reviewed here—the Puffer, Lowe's, and Child Pornography cases—underscore the same critical point from a different point of view. All three cases underscore a basic premise: if users simply review and log the status of an open network and do not illegally access (or damage) that network, then they face little risk of conviction.

1. The Puffer Case: Shooting the Messenger

¶ 53 Computer hacking cases rarely go to trial,[172] so when they do, the press watches them closely. For example, the case of Stefan Puffer attracted quite a bit of publicity. Puffer was indicted on two counts of fraud for wrongfully accessing the Harris County District Clerk's unprotected wireless network.[173] In early 2002, Puffer had been wardriving in Houston when he noticed that the Harris County District Clerk's office had an open, unsecured wireless LAN. As part of an interview with the *Houston Chronicle*,

encrypted); Brown v. Waddell, 50 F.3d 285, 294 (4th Cir. 1995) (holding that pager "clones" used to intercept numeric transmissions to digital pagers constituted unauthorized interception under the ECPA).

[171] This has also been approached from the perspective of trespass to chattels. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069-73 (N.D. Cal. 2000) (protecting eBay from competition under a trespass to chattels theory). *See also* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 39 (2000) (criticizing the application of the trespass to chattels doctrine in cyberspace); Maureen O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561 (2001) (noting the difficulty of "bricks and mortar" analogies in cyberspace).

[172] *See* Paul Elias, *The Case of the Unhappy Hacker*, ZDNET.COM, May 5, 1999, *available at* http://zdnet.com.com/2100-11-514563.html?legacy=zdnn (recounting the story of Nicolas Middleton, who was prosecuted for computer hacking in San Francisco). This Elias article quotes the Assistant U.S. Attorney responsible for the case as saying that almost all cases settle and that, in fact, they had never before had a case go to trial.

[173] Press Release, United States Department of Justice, Local Man Indicted for Hacking into Harris County District Clerk's Office Computer System (July 24, 2002), *available at* http://www.usdoj.gov/usao/txs/releases/July%202002/020724-puffer.htm.

Puffer demonstrated that the Harris County network was open and that the data within it could be accessed by the public.[174] At no time did Puffer compromise any county files.[175] Regardless, upon learning of the vulnerability, the county shut down its wireless network and then informed the FBI of Puffer's actions.[176] In addition, the County hired outside consultants to design an encryption system for the network.[177] In doing so, the County spent more than $5,000, which is the minimum amount required for federal involvement under the CFAA.[178] The United States Attorney prosecuted Puffer for having accessed the network and for "causing" $5,000 in damage.

¶ 54 According to a Department of Justice press release, Puffer faced up to five years in prison and a $250,000 fine for each of the two charges.[179] At trial, the jury acquitted Puffer after deliberating for a mere fifteen minutes.[180] Although Puffer "accessed" the County network, the jury apparently found that (1) he caused no harm, (2) the network was open and unprotected, and (3) the money that the County spent was unrelated to Puffer; instead, the county's action amounted to a security measure akin to installing a lock on a door. Thus, the jury had little difficulty in finding him innocent.[181]

¶ 55 The Puffer case was labeled a "shoot[] the messenger" case by a group of prominent computer-crime defense attorneys who submitted a brief on computer crime to the Senate.[182] The brief was submitted in the context of the sentencing laws, which are widely viewed within the computer-crime defense community as being vague and unfair.[183] Indeed, it is well-settled case law in other disciplines that a perpetrator cannot be liable for additional security measures that individuals take to secure their homes or businesses. Therefore, even if Puffer was considered to have engaged in a criminal act, it was a mistake to hold him liable for the consultancy costs involved in enabling computer encryption on the County system to prevent future access by others.

[174] *See* Rosanna Ruiz, *Computer Expert Indicted in Alleged Hacking*, HOUS. CHRON., July 25, 2002, at A26.

[175] *See* Rosanna Ruiz, *Jurors Acquit Man of Hacking System at District Clerk's Office*, HOUS. CHRON., Feb. 21, 2003, at A26 (noting, however, that Puffer's activity caused considerable embarrassment for the County).

[176] Steve Brewer & Dwight Silverman, *County Cuts off Computer Network*, HOUS. CHRON., Mar. 21, 2002, at A29.

[177] *See* Ruiz, *supra* note 175 (noting that no files were compromised, but the County subsequently spent $5,000 to improve network security).

[178] *See* 18 U.S.C. § 1030(a)(5)(B)(i).

[179] *See* United States Department of Justice, *supra* note 173.

[180] *See* Ruiz, *supra* note 175 (an interview with a juror who said that the jurors "didn't feel [Puffer] intentionally wanted to do damage, but just [wanted] to embarrass").

[181] *Id.* *See also* JOEL MCNAMARA, SECRETS OF COMPUTER ESPIONAGE 268 (2003) (recounting the Puffer case and acquittal).

[182] Response memorandum from the National Association of Criminal Defense Lawyers, the Electronic Frontier Foundation, and the Sentencing Project to the United States Sentencing Commission, Feb. 19, 2003, *available at* http://cyberlaw.stanford.edu/about/cases/1030%20Comments%202-19-03.pdf.

[183] *See id.* *See also* Robert Lemos, *Lawyers: Hackers Sentenced Too Harshly*, CNET NEWS.COM, Feb. 20, 2003, *available at* http://news.com.com/2100-1001-985407.html?tag=fd_top (describing the memorandum filed by the National Association of Criminal Defense Lawyers et. al., as well as the position of others who take the view that hacker sentencing is too harsh).

2. The Lowe's Case

¶ 56 The Lowe's case is another high-profile case, though it differs greatly from the Puffer case in both scope and intent. In November 2002, federal officials accused two men in Michigan of repeatedly cracking the nationwide network of the Lowe's chain of home improvement stores from their car while parked outside a Lowe's store.[184] The press labeled the act "wardriving,"[185] although the allegations appear to be much more serious: the two men were charged with penetrating and intentionally damaging a Lowe's system in violation of the CFAA. According to an affidavit filed by an FBI investigator, the men accessed the Lowe's Wi-Fi network at a store in Southfield, Michigan, and used the store's network to access the company's central data center at its North Carolina headquarters.[186]

¶ 57 As of June 2004, the case is ongoing, and the only information available is that reported in the press.[187] Until the case makes its way through the legal system, let us assume the information stated above is true. At the outset, it is clear that two major aspects distinguish this case from a "typical" wardriving scenario. These distinctions are critical to understanding why the press and law-enforcement officials should be careful about equating computer crime with wardriving.

¶ 58 First, the men apparently returned to the store parking lot at least six times over a two-week period and accessed store networks at several other Lowe's locations around the country, including stores in Kansas, North Carolina, Kentucky, South Dakota, Florida, and California. If true, this information indicates that the men did not simply record the presence of an open network and move on (a typical wardriving scenario), rather they went on to penetrate other areas of the core corporate network. Access in this regard is not wardriving; instead, such activity is characteristic of traditional cases of unauthorized access.

¶ 59 Second, this case involves allegations of damage, for the men are said to have deployed unspecified hacking software (*i.e.,* some sort of "Trojan horse") at some of the stores, which in one case crashed the point-of-sale terminals at a Lowe's in Long Beach, California.[188] If such allegations are true (*i.e.* if the men damaged the functionality of the network in any way), they could be held liable for such damage under either criminal or tort theories, irrespective of the manner in which the men gained access to the network.

[184] *See* Kevin Poulsen, *Wireless Hacking Bust in Michigan*, SECURITYFOCUS, Nov. 12, 2003, *available at* http://www.securityfocus.com/news/7438.

[185] David Ashenfelter, *Waterford Men Hacked Store Files, FBI Alleges,* DETROIT FREE PRESS, Nov. 11, 2003, *available at* http://www.freep.com/news/locoak/nhack11_20031111.htm (describing the charges against the men, associating their acts with wardriving, and calling wardriving a "recent hacker craze").

[186] *See id.*

[187] In June 2004, the defendants were convicted in a plea bargain arrangement. This supports the arguments made in this section, *i.e.*, that the defendants' acts constitute crimes under existing fraud laws. *See* Kevin Poulsen, *Wardriver Pleads Guilty in Lowes WiFi Hacks*, SECURITYFOCUS, June 4, 2004, *available at* http://www.securityfocus.com/news/8835 (describing the plea bargain for one of the defendants and the associated conviction for fraud).

[188] *Id.*

3. The Child Pornography Case

¶ 60 A Canadian case illustrates yet another way that wardriving can be mistaken for other crimes. In November 2002, a man was caught driving naked from the waist down while watching child pornography on his laptop. The press has reported that this is the first man in Toronto to be charged with stealing an Internet connection.[189]

¶ 61 Again, assuming the aforementioned information is true, the man's actions unquestionably constitute a crime. However, as in the *Lowe's* case, authorities can use existing laws and legislation (here, legislation regarding child pornography and theft of services) to deter and prosecute such behavior. Nonetheless, the press has mistakenly labeled this case as an example of "war driving." For example, the *Toronto Sun* stated that "[s]tealing internet signals, or war driving as it is sometimes called, is becoming more and more common among perverts trying to avoid online detection."[190] The press has seemingly confused the *identification* of open wireless sites—wardriving—with the subsequent access and use of these services to view child pornography. Although describing the case in this manner raises the awareness level of people who have open wireless networks and rightfully illustrates a shocking example of what can happen on an unprotected network, labeling this criminal act as wardriving does a disservice to the many well-intentioned wardrivers who make no effort to access the networks they identify.

4. Proposed State Legislation

¶ 62 Conflicting views about wardriving have led to efforts by state legislators to clarify its legality. Legislators in New Hampshire have introduced a bill that would elucidate rules and regulations that affect the legality of wardriving.[191] House Bill 495 would absolve users of liability when they inadvertently access networks that are left unsecured by their owners.[192] In short, if an owner leaves a network open, state law will assume that the owner intends to share access to that network with others, free of charge. Some commentators believe that this bill, if passed, will have no effect since it duplicates existing legislation.[193] Regardless, the proposed bill indeed highlights widespread concerns about wardriving and its implications. Such legislative action would be unnecessary if law enforcement could properly distinguish between wardriving and the collateral activities of access and use.

[189] Bradley, *supra* note 8.

[190] *Id.*

[191] *See* An Act Relative to Unauthorized Access to a Wireless Computer Network, H.B. 495, 2003 Leg., 158th Sess. (N.H. 2003), *available at* http://www.gencourt.state.nh.us/ legislation/2003/HB495.html.

[192] *Id.* House Bill 495 has been called the first in the United States to provide legal protection to wardrivers. Brian McWilliams, *Licensed to War Drive in N.H.*, WIRED, Apr. 29, 2003, *available at* http://www.wired.com/news/wireless/0,1382,58651,00.html.

[193] Orin Kerr, a contributor to the well-known legal blog "the Volokh Conspiracy," provided a concise—but effective—analysis of the bill that disagreed with the WIRED analysis (*supra* note 192), and concluded that the Bill will have very little legal effect beyond existing law. *See* Orin Kerr, Would a New Hampshire Bill Really Legalize War Driving?, *at* http://volokh.blogspot.com/ 2003_04_27_volokh_archive.html#200223941 (last visited Jan. 19, 2004).

V. Bluejacking

¶ 63 As with wardriving, bluejacking provides obvious examples of the kinds of problems linked to how open wireless technologies are accessed and used. Bluetooth, like Wi-Fi, is an unlicensed wireless product that is used for the transmission of data between devices. The commercial success of Bluetooth has been somewhat overshadowed by its more powerful Wi-Fi sibling,[194] although Bluetooth is being used more and more for certain devices, particularly mobile phones.[195] Like Wi-Fi, Bluetooth has some inherent security problems, and the exploitation of these problems led to the creation of another unusual activity (and the development of an unusual term for it) called "bluejacking." When a user bluejacks, she takes advantage of a built-in feature of Bluetooth phones that allows people to send information to each other. Bluetooth phones can automatically set up links with other similar devices, and a bluejacker sends (often anonymously) a message or a digital picture to others who have similar devices.[196]

¶ 64 Today, bluejacking is limited to sending and receiving pictures and notes. Unlike with Wi-Fi, bluejackers do not hack into the devices within their range (typically about 30 feet)[197] and download data from those devices.[198] Nonetheless, bluejacking introduces new ethical and legal problems. Although some bluejackers send innocuous messages to people (e.g., "you've been bluejacked!"),[199] others send pornographic pictures. In one case, pornographic pictures were sent to devices in a department store and were viewed by a minor.[200] Displaying pornographic pictures to minors is, of course, illegal.[201] In the future, commercial spam, called "bluespamming,"[202] may be sent in the same way.

[194] *See* Pui-Wing Tam, *The Other Wireless Technology: It's Not Getting the Hype of Wi-Fi, but Bluetooth is Showing up in a Surprising Number of Devices,* WALL ST. J., Mar. 31, 2003, at R8 (discussing the product's slow uptake rate but noting that Bluetooth technology can now be found in printers, camcorders, handheld computers, and mobile phones).

[195] A typical Bluetooth application is the hands-free earpiece that allows people to have their phones in their pockets or elsewhere. The earpiece maintains a wireless connection with the mobile phone using Bluetooth technology.

[196] *See* Matt Moore, *Cell Phone Messaging Turns Mischievous*, SILICONVALLEY.COM, Nov. 13, 2003, *available at* http://www.siliconvalley.com/mld/siliconvalley/news/7245662.htm (describing bluejacking activity in Sweden). *See also* Jennifer L. Schenker, *A New Way to Say, "Hello, it's Me,"* INT'L HERALD TRIB., Nov. 17, 2003, at 8 (describing cases of bluejacking in London's train stations).

[197] *See* Chris Tomlinson, *E-Business: Beware the Bluejackers Homing in on Your Visible Signal*, BIRMINGHAM POST (UK), Dec. 16, 2003, at 22 (noting the 30-foot distance of Bluetooth devices and discussing the increasing practice of bluejacking in Birmingham).

[198] See Gordon Collins, *Bluetooth Security Needs More Bite*, INFO. SYS. AUDITOR, June 1, 2003, at 1 (describing the different "modes" of Bluetooth technology and noting that certain modes are more "hackable" than others).

[199] *See Hello Handsome, You've Just Been Bluejacked*, BUS. TIMES ONLINE, Nov. 17, 2003, *available at* http://business-times.asia1.com.sg/story/0,4567,99907,00.html.

[200] *See* Maheesha Kottegoda, *Horrified Dad Finds Porn Pix on Store's Mobile Phone*, IC SURREYONLINE, Dec. 31, 2003, *available at* http://icsurreyonline.icnetwork.co.uk/0100news/0200surreyheadlines/page.cfm?objectid=13770915&method=full&siteid=50101 (recounting the story of a father and his child who spotted photographs of genitals on a phone at a department store).

[201] *See, e.g.,* Commonwealth v. Anderson, 550 A.2d 807, 810 (Pa. Super. Ct. 1988) (discussing prosecution for "corruption of minors," where pornography was displayed to a minor).

[202] *Companies Face Customer Backlash over Bluejacking, Warns Technology Agency Rainer PR,* M2 PRESSWIRE, Nov 25, 2003 (noting that by 2004, 20% of all phones sold are expected to incorporate

¶ 65 Some websites discuss various ways to bluejack, and at least one website highlights problems posed by the practice and proposes some guidelines.[203] Discussing these issues charts new territory, since the newer handsets that support Bluetooth are only just now coming to market. There is very little sector-specific regulation, and in some countries, it is not even clear who would be assigned regulatory responsibility. In the United States, the FCC regulates some aspects of wireless content for wireless broadcasters,[204] but private communications do not receive the same level of First Amendment protection as public communications.[205]

¶ 66 While a more in-depth discussion of constitutional issues is beyond the scope of this article, bluejacking is an excellent example of the emerging problems associated with the proliferation of open wireless technologies, for such activities cover access as well as content. We saw earlier that derivatives of wardriving have resulted in prosecutions for downloading child pornography,[206] and the press reports that bluejacking has raised content issues, such as pornography, that regulators and law-enforcement officials will need to address.[207] Europe is well ahead of the United States in promoting laws and regulations addressing wireless ethics, particularly as such ethics relate to minors.[208] Although 3G[209] services are not yet widely available in the United States,[210] in Europe, the newer services offered by 3G are often referred to as "Girls, Gambling and Games,"[211] and industry regulation is a growing concern.[212] For now, European industry

Bluetooth chips and that this number is expected to increase to 75% by 2008). This article suggests that bluejacking may be a new phenomenon for use by marketing agencies and spammers.

[203] *See* http://www.bluejacking.info/index.html (last visited Jan. 7, 2004). *See also* http://www.bluejackq.com/howto (last visited Jan. 7, 2004) (a popular "how to" bluejacking site that gives instructions on the practice but that does not provide ethical guidelines, boasting that "the rest, they say, is up to you").

[204] *But see* Jeffrey S. Hurwitz, Note, *Teletext and the FCC: Turning the Content Regulatory Clock Backwards*, 64 B.U. L. REV. 1057, 1058 (1984) (noting that the FCC chose not to regulate teletext as a form of broadcasting).

[205] The Supreme Court has often highlighted this dichotomy between state and private action by arguing that the 14th amendment erects no shield against merely private conduct, "however discriminatory or wrongful." Jackson v. Metropolitan Edison Co., 419 U.S. 345, 349 (1974) (quoting Shelley v. Kraemer, 334 U.S. 1, 13 (1948)).

[206] *See* Bradley, *supra* note 8.

[207] *See* Kottegoda, *supra* note 200 (noting the sending of pornography through Bluetooth signals).

[208] *See generally* Programme for the Children, Mobile Phones, and the Internet Experts' Meeting at the Mitsubishi Research Institute, Tokyo (Mar. 2003), *available at* http://www.iajapan.org/hotline/2003mobilepro-en.html (containing the proposals and slides from various regulatory and industry experts in Europe and Japan that present the problem of protecting children in the mobile-phone sector).

[209] 3G is short for Third Generation Mobile Telephony, a high bit-rate service that is expected to provide several mobile video and data services to customers. *See* http://www.fcc.gov/3G/ (last viewed July 1, 2004) (defining 3G and its intended purpose).

[210] New frequencies are recently being made available for "Advanced Wireless Services" that will cover many 3G uses. *See generally* Patrick S. Ryan, *Wireless Spectrum Allocation and New Technologies: Reviewing Old and New Paradigms Through a Case Study of the U.S. Ultra Wideband Proceeding*, 2002 GERMAN WORKING PAPERS IN LAW & ECON. No. 8., *available at* http://www.bepress.com/gwp/default/vol2002/iss1/art8 (noting the delay of 3G deployment in the United States and discussing alternate technologies that are being developed).

[211] *See, e.g.*, Marc van Impe, *3G Stands for Girls, Gambling and Games*, NORDIC WIRELESS WATCH, Feb. 25, 2002, *available at* http://www.nordicwirelesswatch.com/wireless/story.html?story_id=1333 (noting that pornography and gambling are big Internet industries and that such

appears to have chosen to combat the problem through self-regulation, including the creation of special filters that control Internet access by minors.[213] Similarly, U.S. companies Cisco, Intel, Microsoft, and Apple have united to develop security standards to quell consumer access fears regarding Wi-Fi products.[214] This type of industry standardization would please former Security Adviser Richard Clarke, who encouraged manufacturers to find their own solutions (see discussion *infra).* In the future, regulations will probably continue to be a mixture of industry initiative and government action.

VI. THE BATTLEGROUND FOR ETHICAL CODES

¶ 67 Although the debate surrounding wardriving and wireless hacking may seem fairly complex, it is important to note that ethics can play a particularly important role in differentiating computer crimes from innocent activities. Although "hacking" is often synonymous with computer crime,[215] the two are in fact very different.[216] Those who walk the line that separates innocent activity from crime are called "gray-hat hackers," which denotes hackers with questionable ethics.[217] This unusual term found its way into hacking vernacular, not surprisingly, via Hollywood. In black-and-white movie Westerns, the bad guys wore black hats and were easy to distinguish from the good guys, who wore white hats.[218] Unlike the old Westerns, little is black and white in today's increasingly Internet-reliant society.

¶ 68 An example may shed some light on the ethical dilemmas posed by gray-hat hacking. One self-proclaimed gray-hat hacker, who runs a security firm called SnoSoft,

sources of income lend themselves naturally to 3G, for which European operators paid billions for licenses and must now find new profitable applications to recuperate their investments).

[212] *See* Robert Budden, *Mobile Operators Draft Code on Access to Porn*, FIN. TIMES, Aug. 8, 2003 (discussing a draft "code of practice" among mobile operators that may classify certain material for viewing only by people over the age of eighteen).

[213] *See* David Batty & Justin McCurry, *Children to Be Shielded from Abuse via Mobiles,* GUARDIAN, Jan. 12, 2004, *available at* http://www.guardian.co.uk/online/story/0,3605,1121078,00.html (discussing a new regulation, agreed to by the six largest mobile phone operators in the UK—Orange, O2, T-Mobile, Virgin, Vodaphone, and 3—that will stop children from entering chat rooms, accessing porn sites, and using gambling services).

[214] *See* Glenn Fleishman, *Key to Wi-Fi Security*, INFOWORLD, Jan. 10, 2003, *available at* http://www.infoworld.com/article/03/01/10/030113newifisec_1.html.

[215] *See* Briggs v. State, 704 A.2d 904, 907 n.4 (Md. 1998) (defining a "hacker" as a "computer user who intends to gain unauthorized access to a computer system," and noting that the term "hacker" has "become synonymous with a computer criminal, and typically refers to a person who breaks into computer networks").

[216] *See Revenge of the Hackers*, ECONOMIST, July 11, 1998, at 63 (describing the open-source movement Linux and describing its pioneer, Linus Torvalds, as a "hacker").

[217] *See* Wible, *supra* note 57, at 1621 (discussing gray-hat hacker ethics).

[218] *See* Jude Thaddeus, *The Confessions of a White Hat Hacker*, COMPUTERWORLD, Dec. 4, 2000, *available at* http://www.computerworld.com/printthis/2000/0,4814,54616,00.html (discussing gray-hat hacker ethics and explaining the Hollywood roots of the term); John O'Connell, *Battling the Invaders*, IDAHO ST. J., Dec. 7, 2003, *available at* http://www.journalnet.com/articles/2003/12/07/features/living/living01.txt (noting the Western movie roots of the terms and specifying that a "gray hat protects computers and doesn't mind bending a few rules").

alerted Hewlett Packard (HP) to security vulnerabilities in the company's system.[219] Instead of hiring SnoSoft to fix the problem, HP understandably chose to fix the error itself. However, when a SnoSoft employee posted the vulnerability information to a reputable Internet site used for reporting known bugs and other problems,[220] HP threatened Snosoft with a lawsuit under the Digital Millennium Copyright Act (DMCA).[221] The HP letter to SnoSoft is reproduced in its entirety on a well-known computer law and politics website.[222] HP's threat shot like a bullet through the Internet.[223] Under massive pressure from users, hackers, and policy organizations, HP quickly reconsidered its actions and published an unprecedented public retraction:

> Where and how the DMCA should be applied is a matter of great controversy. The reported letter to SnoSoft was not consistent or indicative of HP's policy. We can say emphatically that HP will not use the DMCA to stifle research or impede the flow of information that would benefit our customers and improve their system security.[224]

¶ 69 This exchange highlights the ethical tensions that exist among users, hackers, and large software companies, all of whom wear hats of varying shades and styles. The HP case illustrates the dilemmas faced by computer companies who choose not to hire computer security firms for fear that doing so on a regular basis would invite commercial hackers to seek flaws. The exchange also shows the ability and willingness of the hacking community to respond to the largest of corporations, especially when those large corporations enact controversial measures to quash the publication of vulnerabilities, a sacred cow in the hacking community. Indeed, the swift and clearly negative public reaction to HP's litigiousness is not unlike the Puffer jury's fifteen-minute acquittal of the defendant, who also identified and published a network vulnerability. Both Puffer's

[219] *See* Robert Lemos, *When Is Hacking a Crime?* ZDNET.COM, Sept. 23, 2002, *available at* http://zdnet.com.com/2100-1105-958920.html (discussing the actions taken by SnoSoft to report the vulnerabilities to HP and the threat that SnoSoft received as a result).

[220] The site was a mailing list for SecurityFocus.com called "Bugtraq." *See* http://www.securityfocus.com/popups/forums/bugtraq/faq.shtml (last visited Jan. 15, 2004).

[221] *See* Lemos, *supra* note 219. The DMCA has been battered with criticism. Stanford cyber-crime defense lawyer Jennifer Granick has convincingly argued that "the problem with the DMCA is it doesn't make intuitive sense to people who are practicing in this field, so even after reading the statute, people don't understand exactly what they are or aren't allowed to do." Kevin Poulsen, *Linux Update Withholds Security Info on DMCA Terror*, REGISTER, Oct. 30, 2001, *available at* http://www.theregister.co.uk/2001/10/30/linux_update_withholds_security_info/print.html (quoting Jennifer Granick, director of Stanford Law School's Law and Technology Clinic).

[222] *See* Letter from Kent Ferson, HP, to Adriel T. Desautels, Secure Network Operators, Inc. (July 29, 2002), *available at* http://www.politechbot.com/docs/hp.dmca.threat.073002.html.

[223] *See* Brad Levang, *Hewlett Packard's Troubling Attempt to Use the Digital Millennium Copyright Act in the Computer Security Context,* FINDLAW, Aug. 14, 2002, *available at* http://writ.news.findlaw.com/student/20020814_levang.html; Declan McCullagh, *Security Warning Draws DMCA Threat*, CNET NEWS.COM, July 30, 2002, *available at* http://zdnet.com.com/2100-1104-947325.html; Brian McWilliams, *HP Exploit Suit Threat Has Holes*, WIRED, Aug. 2, 2002, *available at* http://www.wired.com/news/ technology/0,1282,54297,00.html; Kim Zetter, *HP, Bug-Hunters Declare Truce*, PCWORLD.COM, Aug. 9, 2002, *available at* http://www.pcworld.com/news/article/0,aid,103853,00.asp.

[224] *See Document: HP Backs Off DMCA Threat*, CNET NEWS.COM, Aug. 1, 2002, *available at* http://news.com.com/2100-1023-947740.html (publishing the HP statement).

acquittal and the HP retraction show that the publication of network vulnerabilities has been judged ethical by the court of public opinion.

¶ 70 In the heat of this controversy, Richard Clarke, former Special Presidential Adviser on Cyberspace Security, captured these ethical tensions in a comment made in a 2002 speech at a prominent meeting (ironically, called a "Black Hat Security Conference"[225]): "There are a lot of people in our country that rely on cyberspace, who are not taking responsibility for securing their part of cyberspace."[226] An important question remains: *who* should take responsibility for security: users, manufacturers, or both? The answer is both, *sort of.* After all, existing laws impose high penalties on those who inform network owners of vulnerabilities, and highly controversial cases have arisen involving hackers who exposed security holes, which raises difficult First Amendment problems.[227] Users, who are sometimes indistinguishable from hackers,[228] may believe that they are good cyber-citizens but risk prosecution or civil liability when they use email to inform fellow users of a product about security problems,[229] or when they publish software vulnerability information on the Internet.[230] Nonetheless, network operators and software manufacturers depend heavily on their customers and users to

[225] The Black Hat Security Conference is one of many hacker conferences, and perhaps one of the more controversial. As its name may suggest, it has been considered by some as a "burglar school." *See* Larry Seltzer, *Black Hat: Security Conference or Burglar School?* EWEEK, July 31, 2003, *available at* http://www.eweek.com/article2/0,4149,1239111,00.asp.

[226] Robert Lemos, *Security Czar Points Finger of Blame*, CNET NEWS.COM, July 31, 2002, *available at* http://zdnet.com.com/2100-1105-947409.html (quoting Richard Clarke).

[227] *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445 (2d Cir. 2001), *aff'g* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000). Corley published the DeCSS program as part of a hacking article. The lower court found that this distribution of the code violated the DMCA's prohibition on trafficking in anti-circumvention programs, and on appeal, Corley argued that the DMCA violated his First Amendment rights of free speech. *Corley*, 273 F.3d at 436. Corley claimed that he had a First Amendment right to publish the code as protected speech and that he was not directly involved in any copyright infringement himself. The Second Circuit recognized that computer programs can be protected speech but that in this particular instance the program was primarily functional. *Id.* at 455. *See also* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1142 n. 200 (1998) (arguing that copyright's fair use doctrine creates an affirmative right to hack technical protection systems to make fair uses).

[228] The publication of a software vulnerability can take many forms, sometimes just by users who discuss a problem in a chat room or who post a question on a blog. Software users may wish to make (legal) changes to certain programs so that the programs can interoperate with other software that they use. The process of making these changes is also called "hacking."

[229] A classic gray-hat example: an employee who worked for a software company discovered a vulnerability in the software and informed his employer about it. The company chose to do nothing, and the employee quit. Afterwards, the employee sent an email to customers of the company and informed them of the security vulnerability. The company spent more than $5,000 in contacting the customers and in fixing the vulnerability, which triggered the $5,000 damage requirement under former 18 U.S.C. § 1030(a)(5) (2000). As a result, the Federal Government successfully prosecuted the employee under this provision, resulting in a sixteen-month jail term. After the employee served the entire sentence, on appeal (the appeal took place during and after the sentence was served), the government realized that there were several problems with the conviction and filed a motion to reverse the conviction. *See* Government's Motion for Reversal of Conviction, U.S. v. McDanel (9th Cir. 2003) (No. 03-50135), *available at* http://www.steptoe.com/publications/273a.pdf; Robert Lemos, *Feds Admit Error in Hacking Conviction,* CNET NEWS.COM, Oct. 16, 2003, *available at* http://zdnet.com.com/2100-1105-5092697.html.

[230] *See Reimerdes*, 111 F. Supp. 2d at 312 (publication of DeCSS in *The Hacker Quarterly*).

provide feedback in order to identify security holes, bugs, and other problems.[231]

¶ 71 It is apparent that there is no clear consensus on how to share information about security holes. Everyone agrees that some type of publication component is vital, but the parties differ on the details as to *when, where,* and by *whom* these vulnerabilities should be published. Large equipment manufacturer Cisco[232] sells security consulting services and posts the details of vulnerabilities for all kinds of products on the Internet.[233] As seen in the HP/SnoSoft exchange, smaller security services also publish vulnerabilities on the Internet, and many of these companies are no less reputable than Cisco. Nonetheless, there appears to have been many more cases filed—both tort[234] and criminal[235]—against individuals and small companies for publishing system vulnerabilities than against large companies. It is unlikely, for example, that HP would have sent a threatening letter to a company the size of Cisco.

¶ 72 For hacking, size and stature clearly matter.[236] A low-tech hacking incident further illustrates this point. When an admissions official at Princeton University "hacked" into servers at fellow Ivy-League school Yale University to view its admissions

[231] Microsoft XP has a built-in bug-reporting system that will automatically inform Microsoft of bugs and failures. The customer chooses to allow her computer to report the bug to Microsoft on a per-occurrence basis. This process shows that many bugs are discovered as a result of customer feedback, and the company regularly posts "security bulletins" and patches for its software. There is an ongoing debate as to whether or not Microsoft should force its customers to accept patches. AOL users, for example, complained heavily when they were forced to accept lengthy, mysterious updates when logging off their machines. *See* Scott Spanbauer, *Microsoft's Patch Policy Pickle,* PC WORLD, Nov. 2003, *available at* http://www.pcworld.com/news/article/0,aid,112747,00.asp; Paul Roberts, *Microsoft Revises Bug Alerts*, PC WORLD, Oct. 23, 2003, *available at* http://www.pcworld.com/news/article/0,aid,113084,00.asp.

[232] *See* Scott Thurm, *Boss Talk: How to Drive an Express Train*, WALL ST. J., June 1, 2000, at B1 (stating that in 2000 Cisco reached a market capitalization of $541 billion, making it the third most valuable company in the world).

[233] Cisco's division for security services, called Cisco Secure Consulting Services (CSCS), publishes an online "encyclopedia" with vulnerability information on products from various manufacturers. *See* http://www.cisco.com/pcgi-bin/front.x/csec/csecHome.pl (last visited Jan. 14, 2004). Carnegie Mellon's Software Engineering Institute also offers an exhaustive catalogue of vulnerabilities and has signed agreements with the U.S. government to provide cyber-threat advice. *See* CERT Coordination Center, *available at* http://www.cert.org (last visited Jan. 14, 2004).

[234] *See, e.g.,* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (suit included tort claim against the publisher of *The Hacker Quarterly* for publication of DeCSS).

[235] One of the most famous cases was *United States v. Neidorf*, in which the publisher of *Phrack* magazine, Craig Neidorf, downloaded and published material on the E911 system. He was brought to trial on several felony counts, but five days into testimony, when experts showed that this same information was freely available in the public domain, the government dropped the charges. Although Neidorf was never convicted, he nonetheless had to pay more than $100,000 in attorney fees and faced the possibility of more than 50 years of imprisonment. *See* Denning, *supra* note 55. *See also* United States v. Riggs, 743 F.Supp. 556 (N.D. Ill., 1990) (criminal case against the publisher of *Phrack* magazine).

[236] Large companies like Microsoft, Symantec, Oracle, and others are working closely with the non-governmental Organization for Internet Security to put pressure on individuals and small companies to prevent hackers from publicizing holes. *See* Joseph Menn, *Going by the Rules with Software Flaws*, SEATTLE TIMES, Nov. 29, 2003, *available at* http://seattletimes.nwsource.com/html/businesstechnology/2001803207_msflaws290.html (noting the alliances and a proposed one hundred-step code).

decisions,[237] the FBI investigated the matter to see if any federal laws—specifically the Buckley Amendment—were violated.[238] Ultimately, Princeton undertook its own disciplinary measures, including the removal of its admissions director.[239] The Princeton case is particularly scandalous when viewed in an academic context, since the academic world, and Princeton in particular, is bound by long traditions of ethical codes of honor.[240] Indeed, expulsion from the system (*e.g.,* removal of the official from his position) is perhaps the best punishment for such a violation. In many ways, the Princeton response provides a model for how hackers might deal with their own when a serious ethical violation occurs.

¶ 73 The problem is that there is neither a tradition of hacking ethics nor a single code of honor. This vacuum creates room for external forces to determine how to respond or proceed when an ethical dilemma arises. Thus, the wheels of justice turn quite differently for different people. For example, a hacker who posts or notifies an operator of a system vulnerability may face state intervention and jail time.[241] Alternatively, she may be held civilly liable (as HP has threatened), or she may just lose her job.[242] On the other side of the spectrum, it is also possible that she may be rewarded for her hacking efforts.[243] This

[237] Princeton admissions officials were found to have used the information of certain applicants (name, birth date, and Social Security Number) to access their admission decisions on Yale's online system. *See* Elise Jordan & Arielle Levin Becker, *Princeton Officials Broke into Yale Online Admissions Decisions*, YALE DAILY NEWS, July 25, 2002, *available at* http://www.yaledailynews.com/article.asp?AID=19454.

[238] The FBI chose to investigate the matter, and Princeton's associate dean and director of admissions were put on a leave of absence during the investigation. *See* Elise Jordan & Arielle Levin Becker, *FBI to Investigate Princeton Admissions Hacking Incident*, YALE DAILY NEWS, July 26, 2002, *available at* http://www.yaledailynews.com/article.asp?AID=19455; *Top US Colleges in Hacking Row*, BBC NEWS, July 26, 2002, *available at* http://news.bbc.co.uk/1/hi/world/americas/2153287.stm.

[239] Silla Brush & Zach A. Goldfarb, *LeMenager Removed for Yale Web Breach*, DAILY PRINCETONIAN, Sept. 11, 2002, *available at* http://www.dailyprincetonian.com/archives/2002/09/11/news/5240.shtml.

[240] *See, e.g.,* Princeton Honor Code (2000), *available at* http://www.princeton.edu/~honor/constitution.htm. Changes to the Honor Code require approval by various committees and juries and can often be controversial. *See* Catherine Farmer, *Proposed Code Change Harms 'Spirit' of Deliberations*, DAILY PRINCETONIAN, Apr. 11, 2003, *available at* http://www.dailyprincetonian.com/archives/2003/04/11/opinion/7895.shtml.

[241] In the Puffer case, an individual notified a network operator of the lack of protection in the network. He was rewarded with federal prosecution. Although the jury acquitted him, the case illustrates the problems involved in discovering and reporting security flaws. *See* discussion *supra* at Section IV. *See also* discussion *supra* note 229 regarding *United States v. McDanel*, where a hacker who notified customers of a security problem was convicted and subsequently served sixteen months in jail. Also, an early-1990s phenomenon known as "the hacker crackdown" led to multiple federal prosecutions and the emergence of the Electronic Frontier Foundation (EFF), which defended many hackers and online liberties. *See* Bruce Sterling, *The Hacker Crackdown*, LAW & DISORDER ON THE ELECTRONIC FRONTIER (Texinfo ed. 1.2. 1994) *available at* http://www.instinct.org/texts/the_hacker_crackdown/postscript/crackdown-1.2.ps (describing many criminal prosecutions and the emergence of the EFF). *See also* Electronic Frontier Foundation, Active EFF Legal Cases and Efforts, *available at* http://www.eff.org/Legal/active_legal.html (last visited Jan. 15, 2004).

[242] *See* Brush & Goldfarb, *supra* note 239.

[243] There are various types of rewards. On the one hand, hackers like "Captain Zap" who have been criminally prosecuted are subsequently able to earn profits through security consulting as a result of their fame. See discussion *supra* note 100. On the other hand, hackers can profit from winning various

apparently arbitrary range of outcomes depends somewhat on the law, but it relies even more on different interpretations of ethical principles. These interpretations, in turn, hinge on various beliefs as to where to place the onus for the discovery and reporting of security flaws.

¶ 74 Former national cyber-security adviser Clarke's position has been interpreted as a warning to software makers. He places the onus squarely on their shoulders to secure known vulnerabilities. Furthermore, Clarke has specifically pointed to wireless networks as an area in need of help.[244] The concept of manufacturer accountability is found in other areas of product liability law, such as "lemon laws" that hold automobile sellers accountable for the quality of the cars they put on the market.[245] These laws protect less-powerful consumers from vendors who do not take reasonable precautions to provide defect-free products. But software is unlike automobiles or other manufactured products: it is not inherently dangerous, and it is not possible to test all of the different ways that a program can operate with thousands of other software products. Thus, it is illogical to hold derelict software manufacturers liable in the same way we hold derelict automobile manufacturers liable.

¶ 75 Software manufacturers rely heavily on their users for feedback. Even though some sectors of the software market are essentially dominated by one player,[246] competition is fierce in many other sectors, and pressure to get products on the market quickly often conflicts with the software testing process. As a consequence, many products are launched before they are ready, and patches are then delivered when customers report problems. Thus, traditional product liability proposals and lemon-law analogies cannot be easily applied to the software arena. For example, one can download a patch and fix a software vulnerability in a matter of seconds. On the other hand, correcting a poorly designed vehicle gas tank that can explode and severely injure passengers requires a full product recall.[247]

hacking contests. A contest in 2001 called OpenHack III offered $50,000 to hackers who could penetrate its product. *See* Marni Leff, *$50,000 Prize -- If They can Hack It,* SEATTLE POST, Jan. 16, 2001, *available at* http://seattlepi.nwsource.com/business/hack161.shtml. This contest has stirred up controversy: many who hacked into the system believed that the company refused to pay the reward money. *See* Kevin Poulsen, *"Hacking Challenge" Winners Allege $43,000 Contest Rip-Off,* SECURITYFOCUS, Nov. 26, 2002, *available at* http://www.securityfocus.com/news/1717. However, these hacking contests continue. *See* Paul Roberts, *Hackers Rev Up for Weekend Attack,* PC WORLD, July 2, 2003, *available at* http://www.pcworld.com/news/article/0,aid,111438,00.asp.

[244] In his 2002 speech in Las Vegas, Clarke noted that many companies have wireless LANs that are completely unprotected, and said that the Department of Defense has discontinued their use as a result. *See* Lisa Gill, *U.S. Cyber Security Chief Lambastes Software Makers*, NEWSFACTOR NETWORK, Aug. 1, 2002, *available at* http://www.newsfactor.com/story.xhtml?story_id=18850 (summarizing Clarke's position).

[245] *See A Lemon Law for Software?,* ECONOMIST, Mar. 16, 2002 (describing the "lemon law" proposals for software and noting the many differences in the manufacturing markets and software markets).

[246] *See* United States v. Microsoft Corp., 84 F. Supp. 2d 9, 19 (D.D.C. 1999) (finding that "Microsoft enjoys monopoly power in the relevant market").

[247] *See* Grimshaw v. Ford Motor Co., 174 Cal. Rptr. 348 (reporting the Pinto case: jury verdict of $125 million in punitive damages against an automobile manufacturer reduced on appeal to $3.5 million);

¶ 76 Public disclosure of software vulnerabilities and problems is beneficial to all. Yet in passing the DMCA, the government has created laws that criminalize the conduct of hackers who identify vulnerabilities while in the same breath warning software makers that they must identify—and either debug or otherwise correct—problems with their products. Since individuals and small companies risk prosecution under the DMCA, similar to the threat made by HP against SnoSoft, the burden is shifted to the software makers. The problem is further exacerbated by the ethical (and legal) tensions that already exist between software manufacturers and users. There is also insufficient recognition of the psychological motivations that drive many hackers to seek the challenges inherent in discovering security issues in the first place.[248] Of course, some hackers are also inspired by non-trivial financial motivations as well.[249] All of these factors multiply the ethical questions posed, rendering the debate as colored heavily with shades of gray.

A. Development of Hacker Ethics: A (Brief) Twenty-Year Retrospective

¶ 77 Computing ethics have taken many forms throughout the years. In the early 1980s, well-known manifestos billed as "ethics" touted the individual right to experience pure, uninhibited hacking freedom. Naturally, "freedom" meant different things to different hackers, and it took whatever form hackers thought appropriate by their own standards. Sometimes, this freedom took the form of illegal activities (*e.g.*, damaging data on accessed computers). Fortunately, in the 1990s these hacking ethics (or the lack thereof) began to change, and today the stage is set for hackers to assert rights of self-regulation. Hopefully, hackers will embrace this opportunity to establish guidelines surrounding their (oftentimes controversial) hacking activities.

¶ 78 Recent evidence suggests that hackers are beginning to take an interest in the manner in which they are portrayed in the media, and are striving to gain recognition for their contributions in the world of computing. Predictably, however, hackers' efforts to attain a respectable standing in the computing community have been an uphill battle. Nevertheless, hackers have begun to organize and call attention to their accomplishments, thereby ushering their hacking activities into the mainstream. Every year, for example, hackers organize the DefCon Convention in Las Vegas, a large conference where they share information on vulnerabilities.[250] Before the DefCon Convention, hacker meetings tended to be loosely organized and secretive underground groups with no recognizable ethical values or coherent policies worth sharing with the world, let alone with law enforcement officials.

Gary T. Schwartz, *The Myth of the Ford Pinto Case*, 43 RUTGERS L. REV. 1013 (1991) (analyzing Grimshaw v. Ford Motor Co. and detailing the facts and the procedure).

[248] There are numerous theories on hacking culture, although many believe that there are varied psychological motivations that "will continue to flourish." *See* Marc Rogers, A NEW HACKER TAXONOMY (U. of Manitoba Working Paper), *available at* http://psyber.letifer.org/downloads/priv/hacker_doc.pdf (last visited Jan. 14, 2004).

[249] See discussion *supra* note 243 regarding different types of financial motivations, including hack-in contests and fame earned through hacking that can be parlayed into consulting assignments.

[250] The DefCon Conference has an official website where past programs and other information can be freely accessed. *See* http://www.defcon.org (last visited Jan. 15, 2004).

1. The Post-*WarGames* Hacker's Code of Ethics (Levy, 1984)

¶ 79 Shortly after the release of *WarGames*, author Steven Levy wrote a now-famous book entitled *Hackers: Heroes of the Computer Revolution*.[251] The book, which outlines the history of the hacker generation, starts with the MIT movement in the late fifties, analyzes the first personal computer users of the mid-seventies, and concludes with the (then) new generation "game hackers" of the early eighties. Levy repeatedly argues that a "hacker ethic" is responsible for finding and promoting the best and most efficient code for computer programs. He then promotes the somewhat anarchic "Hacker's Code of Ethics," and contends that access to systems should be "unlimited and total."[252] Levy's contribution to the hacking community was significant because no one had so clearly articulated a "code" before.[253] His Code reads as follows:

> [1] Access to Computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the Hands-On Imperative! . . . [2] All information should be free … [3] Mistrust Authority - Promote Decentralization . . . [4] Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position . . . [5] You can create art and beauty on a computer . . . [6] Computers can change your life for the better.[254]

¶ 80 Despite its noble name, there were very few *ethics* in Levy's Code, with the only possible exception being the non-discrimination statement found in item four (an ethic already engrained in our social structure). Instead, the Code reads like a battle cry. Its proclamation that access should be "unlimited and total" and that "[a]ll information should be free" set no boundaries on hackers whatsoever. Furthermore, the assertion that hackers should "[m]istrust [a]uthority," while debatably a noble mantra, instead encourages hackers to disregard established rules and laws. On the whole, the Hacker's Code of Ethics is ethically bankrupt. Because of its name, however, some commentators have misinterpreted it. One scholar even incorrectly wrote that Levy's Code "prohibited causing damage to any computer or to information."[255] The Code does no such thing.

[251] STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 26-31 (1984).

[252] This code has been reprinted and referred to by many scholars. *See, e.g.*, Wible, *supra* note 57, at 1590 n. 84 (reprinting Levy's Hackers Code of Ethics); Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 U. MO-KC L. REV. 139, 141 (1991); Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43, 60 n.113 (2002).

[253] Stewart Brand, *We Owe it all to the Hippies*, TIME, Mar. 22, 1995, at 54. In a special issue of TIME entitled "Welcome to Cyberspace." Brand credits Levy with introducing the world to the "hacker ethic:" "Nobody had written these down in manifestoes before; it was just the way hackers behaved and talked while shaping the leading edge of computer technology." *Id*.

[254] *See* LEVY, *supra* note 251, at 26-31. The Code is also reprinted on the Internet in various sources. *See, e.g.,* http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/Hackers.Code.html (last visited Jan. 13, 2004).

[255] Joseph M. Olivenbaum, *Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 581 (1997) (reading a prohibition to damage into Levy's 1984 Code). *But see* Cutrera, *supra* note 252, at 141 (discussing Levy's Code and noting that it creates friction with the law and fosters a bad reputation among hackers). *See also* Philip W. Esbenshade, *Hacking: Juveniles and Undeterred Recreational Cybercrime*, 23 J. JUV. L. 52, 54 (2002-2003) (describing hacker ethics in general

¶ 81 To be fair, Levy's goal in writing his book was to document the history of hackers, which he accomplishes with tremendous success. The title of his book labeled hackers as "heroes," a powerful statement that contained certain truths. The Hacker's Code of Ethics has been reprinted and referenced often, and few can deny that it captures the spirit of the era.

¶ 82 Levy's Code was an important beginning. Unfortunately, subsequent codes of ethics proposed by other groups offered little improvement. From the publication of Levy's Code (*i.e.,* around the time of the 1983 release of *WarGames*) through the release of *Sneakers* in 1992, a slow evolutionary—far from revolutionary—trend in ethics began to emerge.

2. The Hacker Manifesto ("The Mentor," 1986)

¶ 83 The ethical discussion advanced little after 1984, as hackers continued to assert their rights to unbridled system access. The "ethic" of mistrusting authority continued and took many forms, one of the most obvious being hackers' fear of criminal prosecution if they used their real names and their subsequent use of aliases. Such rights to anonymity should be preserved within reasonable limits, as commentators have convincingly argued.[256] However, anonymity can detract from the meaningful promotion of an ethic. In other words, when hackers lack an ascribable personal identity, they also lack accountability for their statements and actions.

¶ 84 The Hacker Manifesto, written by a well-known hacker who goes by the alias "The Mentor," is a short essay that, like Levy's Code, is cited frequently on the Internet. The Manifesto (also sometimes called "The Conscience of a Hacker") mimics Levy's Hacker's Code of Ethics, in that it makes no excuses, sets no boundaries, and adopts an arrogant tone:

> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all.[257]

¶ 85 The author has clearly incorporated elements of Levy's Code of Ethics,

terms, the author incorrectly describes Lightman's intentions in *WarGames*, stating that "the hacker in *WarGames* gained unauthorized access not to steal or destroy data, but to see just how far he could get;" actually, it was Lightman's intention to steal a game from a private gaming company).

[256] Julie Cohen has advanced some excellent arguments for the preservation of anonymity in the Internet. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1004-07 (1996); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423-36 (2000) (discussing various aspects and implications of "constitutive privacy").

[257] The Mentor, *The Hacker Manifesto*, Jan. 8, 1986, *available at* http://www.bcr.org/~msauers/documents/manifesto.html (filed under the rubric "Classic Internet Documents") (last visited Jan. 14, 2004). *See also* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 77 (2001) (quoting from the Manifesto and using it as evidence for a proposition that hackers have addictive personalities).

particularly those aspects related to non-discrimination. It is a model in bad press, for it mockingly refers to non-discrimination as his "crime," and it does little to advance the ethical discussion. Instead, the Manifesto chooses to quip about outsmarting others and getting away with it. Immunity to detection, capture, and prosecution is part and parcel of anonymity.

¶ 86 Who is "The Mentor" and why does his Manifesto matter? The Mentor was initially an alias, although Loyd Blankenship has since claimed credit.[258] It was given the ultimate hacker recognition when it was published in *Phrack*,[259] and is mandatory reading in the curricula of Internet courses at many universities.[260]

¶ 87 An alternate proposal to the Hacker Manifesto was published in 1988, entitled "A Novice's Guide to Hacking." This publication attempts to establish some ethical boundaries. It begins by declaring that "[h]ackers should not intentionally damage any system" but then it almost immediately contradicts itself, noting that it is acceptable to "alter system files" if "needed to ensure your escape from detection … Trojan Horses … and the like are *all necessary for your survival*."[261]

¶ 88 Approximately two years after the publication of "A Novice's Guide to Hacking," the Mentor (at that point known to be Loyd Blankenship) saw all of his computer equipment confiscated by the Secret Service as part of an investigation into the alleged hacking of Bell South's computer.[262] In a controversial move, the Secret Service also confiscated the computer equipment of Blankenship's employer, Jackson Games. Since Jackson Games had no connection to Blankenship's allegedly illegal activities, the company sued the Secret Service and obtained a judgment against the government for $42,259 in lost profits and $8,781 in expenses, plus lawyer fees.[263] The decision was highly publicized[264] and copies of the judgment and court documents can be found on hacker websites.[265] Although the decision was not directly related to Blankenship, it

[258] *See* The Hacker's Encyclopedia, *available at* http://www.insecure.org/stf/HackersEncyclope2.0.html (last visited Jan. 15, 2004).

[259] The Hacker Manifesto first appeared in *Phrack*, Vol. 1, Issue 7 (January 1986), *available at* http://www.phrack.org/show.php?p=7&a=3.

[260] The Hacker Manifesto is taught, *inter alia*, at numerous universities, including the University of Southern California (http://www.usc.edu/~douglast/202/lecture23); the University of Texas (http://www.cwrl.utexas.edu/~davis/crs/309/309syllabus.htm); and the University of Kentucky (http://www.uky.edu/~uebel/378.htm (all sites last visited Jan. 15, 2004).

[261] *See* http://www.phrack.org/phrack/22/P22-04 (last visited Jan. 12, 2004) (emphasis added).

[262] *See* Joe Abernathy, *Trial Set this Week in Computer Case*, HOUS. CHRON., Jan. 18, 1993, at A13; Joe Abernathy, *Computer Case Opens*, HOUS. CHRON., Jan. 27, 1993, at A11. Both articles describe the Secret Service's confiscation of Blankenship's computer equipment from his employer for his alleged involvement in a hacking scheme against Bell South. No charges were filed against the employer.

[263] Steve Jackson Games, Inc. v. United States Secret Serv., 816 F.Supp 432 (W.D. Tex. 1993), *aff'd*, Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994).

[264] *See* Joe Abernathy, *Secret Service Is Faulted in Raid on Computer Firm*, HOUS. CHRON., Mar. 17, 1993, at A1 (describing the judgment against the Secret Service).

[265] *See, e.g.*, Steve Jackson Games corporate website, *available at* http://www.sjgames.com/SS/ (includes a detailed history of the lawsuit with numerous links); Reproduction of Search Affidavit for Steve Jackson Games, *available at* http://www.2600.com/secret/sj/sj-cud.html (providing the details of the case) (both sites last visited Jan. 15, 2004).

advanced his image as a hacking hero within the community. Ultimately, he earned a permanent spot in *Phrack's Hacker's Encyclopedia* (a hacker's trophy) for writing the Manifesto, for having his computer equipment confiscated, and for committing many other underworld acts.[266]

¶ 89 Blankenship no longer appears to be active in hacking circles.[267] Still, his Manifesto portrays the rough-and-ready demeanor of the 1980s hacker, and it has had a profound effect on hackers everywhere. As discussed below, in the 1990s hackers would find breaking away from Blankenship's hacking "ethic" to be a difficult task.

3. *The Cuckoo's Egg* and the Emergence of the "Gray Hat Hacker"

¶ 90 In the early 1990s, hackers were a disorganized group with little more than informal and fairly radical battle cries—dubbed "ethics" and "manifestos"—to guide and unite them. The 1989 book *The Cuckoo's Egg* recounts the true story of Cliff Stoll, a Lawrence Berkeley Lab astronomer, who tracked a computer hacker through a complicated labyrinth of computer systems.[268] The book reads like a fictional spy novel and captures the details of a time when hackers experienced their worst public relations problems. Over a period of eleven months, Stoll tracked the hacker as he downloaded sensitive government information from military, satellite, and other government computer systems. The government eventually prosecuted and imprisoned Stoll's hacker for stealing national secrets and for committing high acts of treason.[269]

¶ 91 The book is noteworthy in that it describes in eloquent detail the tools of cyberspace hacking at a time when the public was ready to learn more. *The Cuckoo's Egg* also underscored the public's perception that hackers lacked ethics, and that they were self-serving, arrogant, and malevolent in their intentions. Discussion of the book initiated an earnest, useful debate within the hacker community on the topic of ethics. The perception that all hackers lacked ethical values had begun to wear on the many hackers who did, in fact, live by a moral code. Academics and hackers joined forces in a loose coalition to counteract the negative publicity.[270] The resulting public-relations campaign sent the message that hacking was not a black-and-white pursuit. Well-known hacking publications attacked *The Cuckoo's Egg* for its stereotypical portrayal of hackers:

[266] Like many hacking publications, the Hacker's Encyclopedia, *supra* note 258, is reproduced on various websites and can be found by typing "Hacker's Encyclopedia" in quotation marks in most search engines.

[267] *See, e.g.,* The Hacker's Encyclopedia, *supra* note 258.

[268] CLIFF STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989).

[269] Because the trial of the hacker in question—Markus Hess—took place in Germany (where criminal matters are not public record), the outcome of the trial is not known. However, by most reports, Hess and his accomplices were convicted on various counts. James S. Kunen, *Astronomer Cliff Stoll Stars in the Espionage Game, but for Him Spying Doesn't Really Compute*, People, Dec. 11, 1989, at 118 (describing the indictment of Hess in Germany for selling military computer passwords, software and other data to the KGB). Some sources suggest that Hess and his accomplices were sentenced but did not serve time. *See* http://www.tnellen.com/cybereng/ebooks/hacker.html (last viewed July 1, 2004) (stating that Hess received a 20 month sentence and a fine, but did not serve any time).

[270] The most obvious result of this campaign is the work of Dorothy Denning, described *infra* note 274.

> Stoll's work [in *The Cuckoo's Egg*] is *irresponsible* because his image of the world reminds us of a simpler time, *one where everything sprang from either the forces of light or of darkness.* Hackers are bad: They trash things, are immature, should be punished, and threaten the foundations of hi-tech civilization as we know it. Stoll, on the other hand, is good: He hates hackers, single handedly saved civilization from the modem-macho demons, and fought the good fight as any true he-man would.[271]

¶ 92 The hackers' public-relations campaign received a powerful endorsement when Dorothy Denning, a computer scientist (and later Georgetown professor), wrote an essay that took a friendly view toward hackers.[272] In her essay, Denning shows great respect for the motivations and intentions of hackers. She contends that the hacker discourse "belongs at the very least to the *gray areas* between larger conflicts that we are experiencing at every level of society and business . . ."[273] In the essay, she interviews several hackers, concluding that most are well-intentioned individuals who want to share information as a selfless, goodwill gesture.

¶ 93 The deference and respect that Denning paid to the hacking community helped her paper find its way into many publications, including hacker magazines[274] and law-reviews.[275] In fact, her essay has become one of the most-cited, Internet-available, pro-hacking texts, joining the ranks of Levy's Hacker's Code of Ethics and The Mentor's Hacker Manifesto in its cult status. Like its hacker-written counterparts, Denning's essay can be found in several hundred locations on the Internet.[276] The hacker community began to enjoy some positive public relations exposure, and the drive to establish a set of real hackers' ethics finally started to take hold. Along these lines, the Electronic Frontier Foundation (EFF), which supported civil liberties in the electronic world, was formed.[277] In fact, Denning and the EFF worked together in a famous early case to free a man who

[271] Jim Thomas, *Review of the Cuckoo's Egg*, COMPUTER UNDERGROUND DIGEST, Apr. 27, 1990 (emphasis added), *available at* http://www.skepticfiles.org/hacker/cud106.htm.

[272] Dorothy E. Denning, *Concerning Hackers Who Break into Computer Systems*, 1990 PROC. NAT'L COMPUTER SECURITY CONF. 653, *available at* http://www.cs.georgetown.edu/~denning/hackers/Hackers-NCSC.txt.

[273] *Id.* at 653 (emphasis added).

[274] Denning has often been referred to in the hacking community as a "sympathizer," and she testified as a witness for the defense in the Neidorf trial. For hacker-group discussions and support for Denning, *see* Bruce Sterling, *Afterword: The Hacker Crackdown Three Years Later*, 2600 MAG., Jan. 1, 1994, *available at* http://www.2600.com/secret/sj/sj-sterling1.html (labeling Denning a "hacker sympathizer" and detailing aspects of the "hacker crackdown" that happened in 1990 and 1991 by the federal government).

[275] *See, e.g.*, Wible, *supra* note 57, at 1584 n. 82; Rustad, *supra* note 257, at 70 n.73; Note, *The Criminalization of Copyright Infringement in the Digital Era*, 112 HARV. L. REV. 1705, 1713 n.69 (1999); Haeji Hong, *Hacking Through the Computer Fraud and Abuse Act*, 1998 UCLA J.L. & TECH 1, 8 n.35 (1998).

[276] A search for the following string conducted by the author on Jan. 16, 2004, on google.com resulted in 511 hits: "Concerning Hackers Who Break into Computer Systems." The hits varied widely among academic publications and hacker sources.

[277] *See generally* http://www.eff.org. The EFF has been extremely active for the past fourteen years, and several documents are available on their website. They recently issued a "report card" tracking the status of the DMCA. *See* Fred Von Lohmann, *Unintended Consequences: Three Years under the DMCA*, May 3, 2002, *available at* http://www.eff.org/IP/DMCA/20020503_dmca_consequences.pdf.

was accused of stealing nearly $24,000 in proprietary material and publishing it in *Phrack.* The government dropped the charges after only four days of trial, having been informed by EFF's effective advocacy and Denning's expert witness testimony that the "proprietary" material was freely available in the public domain.[278] Denning's paper and her advocacy efforts made her a legend in hacking communities during the 1990s.[279] In a post-case report, Denning shared an insightful and influential conclusion: greater efforts should be made to teach "computer ethics" in the classroom and in professional forums.[280]

¶ 94 The dialogue that sprung from the publication of *The Cuckoo's Egg*, the founding of the EFF, and supportive actions of Denning and others lead to the maturation of hackers' ethics. The hacker community had formally mobilized, as evidenced in 1996 at the DefCon IV Convention, where the convention's leader announced to the world that the main focus of that year's conference was the "demystification of the hacker image."[281] In a famous postscript document to DefCon IV, its keynote speaker again reinforced the positive image of hackers, even labeling Leonardo da Vinci a hacker for "refus[ing] to limit his exploration of the universe to the constraints his more conventional neighbors called 'the known world.'"[282] In addressing the issue of whether or not hackers are criminals, he wrote:

> Are hackers criminals? . . . The short answer is no, *not necessarily*. Hackers distinguish between real hackers and crackers, or criminal hackers. Crackers use hacking skills to commit fraud, destroy or steal intellectual property, and vandalize the information systems of governments and businesses . . . From here on, though, things get a little vague . . . [however as] life in the next century becomes unimaginably complex, *the skills of hacking will be in demand*. We will need

[278] Denning, *supra* note 55.

[279] Interestingly, in spite of the widespread appreciation among the hacking community for Denning's paper, her deference for hackers was short-lived. Five years later, in 1995, Denning retreated entirely from her 1990 position, stating that her revised view now was that hacking was a "serious problem." She lambasted the hacking community and hackers in general and published a postscript to the 1990 paper, stating that:

> [Hackers] do not distinguish between the dissemination of information about system vulnerabilities and attacks for the purpose of preventing attacks vs. performing them, a distinction that leads to considerably different articles and publications (e.g., CERT advisories vs. Phrack's hacker tutorials). Hackers do not see that in many cases, they are the biggest threat. Were it not for hackers, many systems might never be attacked despite their weaknesses, just as many of us are never robbed even though we are vulnerable.

Dorothy E. Denning, Postscript to "Concerning Hackers Who Break into Computer Systems", Georgetown University, June 11, 1995, *available at* http://www.cs.georgetown.edu/~denning/hackers/Hackers-Postscript.txt.

[280] Denning, *supra* note 55.

[281] Larry Lange*, Trust a Hacker Under 30? You'd Better*, ELEC. ENG'G TIMES, Aug. 19, 1996, *available at* http://www.highbeam.com (subscription required) (quoting the organizer and describing the conference).

[282] Richard Thieme, *Fear and Trembling in Las Vegas* (1996), *available at* http://www.defcon.org/html/TEXT/4/thiemedc4.html (last visited Jan. 18, 2004).

> bushwhackers, pathfinders, scouts. *Hackers who know the territory make good guides on the electronic frontier.*[283]

¶ 95 Thus, a line was drawn in the sand. To survive in the next century, the hackers (*e.g.,* Leonardo da Vinci types, good hackers, pathfinders, and scouts) must distinguish themselves from the criminals (*i.e.,* crackers), for it is the former group whose skills will be sought by commercial enterprises to meet the challenges of posed by the new electronic frontier. Hackers had already seen their hacking grandfathers Kevin Mitnick and Ian Murphy turn their criminal prosecutions into millions through their consulting services.[284] DefCon IV resurrected their images and announced the birth of a commercial hacking era.

B. A Move from Ethics to "Policy"

¶ 96 Having discovered their economic potential, it was now reasonable for hackers to gradually retreat from their anarchist roots and begin to institute self-regulation. However, it has taken a few years for the "demystification" to translate into a formal ethic, and the process continues today. The 1996 DefCon IV convention was a good start. Nevertheless, the effort to develop a formalized code did not gain traction until very recently. A reluctance to embrace the combination of old-school freedoms and new-school commercial ethics caused a few false starts. For example, at a 2000 conference called "Hackers on Planet Earth," an author launched a debate over a unified "Hacker's Code."[285] This debate did little to advance the "ethic," in part because of the extremely wide philosophical net cast in an effort to gain the broadest acceptance possible among blackhat, whitehat and greyhat hackers. Like others before them, the debaters again neglected to exploit a perfectly good opportunity to develop a true ethic.[286] The conference mistakenly sought to unite hackers and crackers at a time when a formal divide was visible between those groups—particularly between hackers with commercial motives and crackers with subversive intents—and it was clear that no single ethic would work for everyone.

¶ 97 Then something unusual and unexpected happened: a true ethic began to emerge. Instead of "ethics" or "manifestos," hackers with commercial motives began to talk of a

[283] *Id.*

[284] There has been great debate on concerning hackers like Murphy who have been reported to earn as much as $500,000 per year today. Kevin Mitnick was prohibited from using computers for three years after his release from prison, a common condition for modern hacker crimes. Mitnick's prosecutors believe that he will make millions from talk-show appearances and ultimately, from computing. *See* Linda Deutsch, *Judge Orders Hacker to Make Token Restitution to Victims,* CINCINNATI ENQUIRER, Aug. 10, 1999, *available at* http://www.enquirer.com/editions/1999/08/10/loc_judge_orders_hacker.html (discussing the conditions of Mitnick's release and the prosecutor's belief that he'll soon be making millions because of his acts).

[285] *See* Brendan Koerner, *Krispy Kremes and Ancient Ethics*, VILLAGE VOICE, Aug. 1, 2000, *available at* http://www.villagevoice.com/issues/0030/koerner.php (discussing the organizer's efforts to formulate a code at the conference).

[286] See *id.* *See also* Steven Mizrach, *Is There a Hacker Ethic for 90s Hackers?*, *at* http://www.fiu.edu/~mizrachs/hackethic.html (last visited Jan. 15, 2004) (an oft-cited, insightful, and comprehensive report on the evolution of the Hacker Ethic).

"policy" or a "disclosure model."[287] Such policies actually read like the ethical codes found in other professions, such as the medical profession[288] or academia.[289] The new hacker policies provide structured guidance and offer a reasonable, good-faith dialogue between the community that embraces them and others like software manufacturers and network owners. One university in Finland set up a website to capture and track policy proposals.[290] The content on the site illustrates the speed with which this new movement is advancing. More than one hundred documents related to the discussion are included on the site, most originating in the last few years.[291]

¶ 98 Discussions surrounding the continued development of a genuine hackers' ethic are in full stride. Leading network security publications have recently begun to call for formalization of the ethic, thereby enhancing the status of the movement. Hackers are seeking what Mark Rasch calls "[a] code of conduct for security specialists with clear guidelines on what they can do when a company or entity refuses to fix a vulnerability."[292] Furthermore, corporate and hacking communities are working hard to create codes of conduct in the form of "win-win" solutions.[293] Exhaustive coverage of the effort is outside the scope of this article;[294] however, a brief overview of some of the

[287] *See* University of Oulu, Vulnerability Disclosure Publications and Discussion Tracking (Feb. 4, 2004), *at* http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/ (listing sources for and against different vulnerability disclosure models).

[288] Hippocrates, a Greek physician in the fifth century BC, developed the "Hippocratic Oath" for physicians, which required each new physician to declare the following: "I will follow that system or regimen which, according to my ability and judgment, I consider for the benefit of my patients, and abstain from whatever is deleterious and mischievous." Hippocratic Oath, *available at* http://scs.student.virginia.edu/~alphaed/hippo.htm (last visited Jan 24, 2004). *See also* Leonard A. Hagen, Note, *Physician Credentialing: Economic Criteria Compete with the Hippocratic Oath*, 31 GONZ. L. REV. 427, 428-29 (1996) (discussing the long-standing Hippocratic principles in health care and applying economic analysis to the present regulation of physicians.)

[289] *See generally* Larry A DiMatteo & Don Wiesner, *Academic Honor Codes: A Legal and Ethical Analysis*, 19 S. ILL. U. L.J. 49 (1994) (discussing academic honor codes).

[290] University of Oulu, *supra* note 287. The website's abstract states:

> A long and vivid debate for and against different vulnerability disclosure models is still taking place. Sources that collect all these valuable arguments are scarce. This [website] acts as a place-holder for related contributions that we are aware of. Papers, articles and more informal documents are grouped based on the type of publication. We hope that these links are useful to anyone familiarising [sic] themselves with the scene or planning further contributions.

[291] *Id.* A manual count of the postings of Revision 1.133 (Feb. 4, 2004) showed that policy proposals were an immensely popular topic in 2001 and 2002. The following tally of documents on vulnerability policies and ethics (including conference papers, journal articles, disclosure policies and guidelines, speeches, books, white papers, and news articles) breaks down as follows: 1980s—no documents; 1990s—seven documents; 2000—twenty-three documents; 2001—forty-eight documents; 2002—forty-four documents; and 2003—fourteen documents.

[292] Mark Rasch, *The Sad Tale of a Security Whistleblower*, SECURITYFOCUS, Aug. 18, 2003, *available at* http://www.securityfocus.com/columnists/179. Rasch describes the Bret McDanel case (see *supra* note 229), and calls for guidelines to avoid such prosecutions in the future. The article was written before the government filed its motion to vacate the McDanel conviction.

[293] Here the term "win-win" is used to describe the collaborative efforts of industry and the hacking community.

[294] *See* Tiina Havana & Juha Röning, *Communication in the Software Vulnerability Reporting Process*, PROC. OF THE 15TH FIRST CONF. ON COMPUTER SECURITY INCIDENT HANDLING, (June 22-27, 2003), *available at* http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST2003-communication/paper.pdf

leading proposals that have emerged offers a heartening sense of the progress made to date. As further evidence of the breakthroughs that have been made, a similar ethic has even emerged for wardriving.

1. Proposed Internet Engineering Task Force Policy (Christey/Wysopal, 2002)

¶ 99 In 2002, Steve Christey and Chris Wysopal submitted a proposal called the "Responsible Vulnerability Disclosure Process" to the Internet Engineering Task Force (IETF).[295] The proposal suggests that hackers and corporations should establish a mutual and flexible vulnerability reporting policy.[296] This would require a hacker who discovers a vulnerability to report it to the vendor or to a reliable third-party coordinator (*e.g.,* a member of the security community). The vendor, in turn, would be required to respond to the notification within seven days. If the software maker's receipt message is automatically generated, the company would be required to provide a date—not to exceed ten days—when it would respond in more detail to the notification. Also, the proposal would require the vendor to update the security researcher every seven days, and try to resolve the vulnerability within thirty days.[297]

¶ 100 What is unique about the Christey/Wysopal proposal is that it is an attempt to formalize a procedure via a prestigious non-governmental organization—the IETF. [298] Potentially, such a forum could be a powerful source for regulation because it is membership-driven and because it has been successful in other areas of Internet regulation, particularly in the setting of standards.[299] The proposal failed, however, and the authors withdrew it from the IETF shortly after submission. Two reasons have been given for the failure: (1) IETF members could not reach consensus over the need for such guidelines, and (2) the proposal was submitted without going through a sometimes complicated and politically complex consultation procedure.[300] As Phil Weiser has pointed out, the IETF is an organization that "move[s] slowly and need[s] to satisfy a

(an excellent overview of the different theoretical proposals for software vulnerability). One of the authors of this conference paper has also written an excellent master's thesis on the topic. *See* Tiina Havana, Communication in the Software Vulnerability Reporting Process (2003) (M.A. Thesis for the Department of Communication and PR at the University of Jyväskylä), *available at* http://www.ee.oulu.fi/research/ouspg/protos/sota/reporting/gradu.pdf.

[295] *See* Steve Christey & Chris Wysopal, Memorandum, Responsible Vulnerability Disclosure Process (2002), *available at* http://www.whitehats.ca/main/about_us/policies/draft-christey-wysopal-vuln-disclosure-00.txt. *See also* Linda Rosencrance, *Bug-Reporting Standards Proposed to IETF*, COMPUTERWORLD, Feb. 22, 2002, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,68558,00.html (describing the Christey/Wysopal Proposal).

[296] *See generally* Christey & Wysopal, *supra* note 295.

[297] *Id.* at 11-12.

[298] For overview of the IETF, see Internet Engineering Task Force, *Overview of the IETF*, *at* http://www.ietf.org/overview.html (last visited Feb. 6, 2004).

[299] Philip J. Weiser, *The Internet, Innovation, and Intellectual Property Policy,* 103 COLUM. L. REV. 534, 542 n. 24 (2003) (briefly describing the functionality of the IETF and providing additional references).

[300] *See* Linda Rosencrance, *Authors Pull Proposal on Bug Reports*, COMPUTERWORLD, Mar. 25, 2002, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,69492,00.html (discussing the withdrawal of the Christey/Wysopal Proposal).

broad range of constituents."[301] Even when the IETF does make policy, "[t]he degree to which [the IETF] can lay claim to representing 'the Internet community' is unclear."[302]

¶ 101 The failure of this policy may be a lost opportunity. In the absence of IETF leadership, other less democratic coalitions, such as the Organization for Internet Safety ("OIS"), are advancing their own policies. OIS industry members include Microsoft, Oracle, Symantec, and others. Presently, the OIS is closed to individuals, but the organization is reconsidering its membership guidelines.[303] The latest policy proposed by OIS was released in the summer of 2003 and is currently under review by industry and the hacking community.[304] The debate over these proposals will undoubtedly lead to much politicking over the coming months. Nevertheless, a consensus seems to be emerging.[305]

2. RFPolicy v. 2.0 (Rain Forest Puppy, 2000)

¶ 102 While the dispute over vulnerabilities slowly progresses through industrial trade groups and non-governmental organizations, an informal, *de facto* policy from mid-2000 has been taking root since the middle of 2000. Almost three years ago, a hacker calling himself "Rain Forest Puppy" posted the "RFPolicy for Vulnerability Disclosure" to a vulnerability-disclosure listserv.[306] This policy is attractive because it comes from a respected hacker who continues to use an alias rather than his real name,[307] and like its industry-based counterparts, it endorses a balance between hacker and industry rights. The policy gives a network owner a certain amount of time (five days) to maintain a dialogue with a hacker who identifies a vulnerability.[308] If a dialogue is maintained, the hacker postpones the publishing of the vulnerability.[309] The policy demands that the hacker show some flexibility regarding the publication date, thus demonstrating recognition that some large companies take longer to generate a patch because the software in question may have many versions, and companies have to consider the side

[301] Weiser, *supra* note 299, at 585.

[302] Kevin Werbach, DIGITAL TORNADO: THE INTERNET AND TELECOMMUNICATIONS POLICY (FCC Office of Plans & Policy, Working Paper No. 29, 1997), *available at* http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf.

[303] The Organization for Internet Safety includes @stake, Blindview, Caldera International, Foundstone, Guardent, ISS, Microsoft, NAI, Oracle, SGI, and Symantec. According to their website, individuals are not allowed to join, although they are "reconsidering that decision." *See* Organization for Internet Safety, *at* http://www.oisafety.org/about.html (last visited Apr. 8, 2004).

[304] Organization for Internet Safety, *Guidelines for Security Vulnerability Reporting and Response, Version 1.0*, July 28, 2003, *available at* http://www.oisafety.org/reference/process.pdf.

[305] *Id.*

[306] Posting from Rain Forest Puppy to Neohapsis Archives, (Jun. 12, 2000), *available at* http://archives.neohapsis.com/archives/vuln-dev/2000-q2/0908.html. This is the posting by the author, Rain Forest Puppy, of his latest policy, v. 2.0. There were also earlier versions of the policy, although as of the date of this publication v. 2.0 was the operational version.

[307] *See generally* Rik Farrow, *The Pros and Cons of Posting Vulnerabilities*, NETWORK MAG., Oct. 1, 2000 (discussing RFPolicy v. 1.1 and the pros and cons of the proposals on the table as of late 2000).

[308] Full Disclosure Policy (RFPolicy) v.2.0, *at* http://www.wiretrip.net/rfp/policy.html (last visited Jan. 14, 2004).

[309] *Id.*

effects and other ramifications of any software fix.[310]

VII. WARDRIVER ETHICS AND WI-FI MANUFACTURER ETHICS

¶ 103 We have seen that codes of ethics place burdens not only on hackers and users, but on manufacturers as well. Manufacturers are beginning to acknowledge this shared responsibility by issuing policy documents for circulation within hacker communities. The guiding principles of wardriving ethics are twofold: wardrivers should behave responsibly and ethically, and manufacturers should be held accountable for protecting consumers and WAP owners from attacks.

A. Wardriver Ethics

¶ 104 Policies and ethics regarding wardriving are slowly emerging. One hacker/wardriver has issued a document, the "Stumbler Code of Ethics v0.2," which addresses wardriving and warchalking.[311] Most of the document offers common-sense guidance about the importance of obeying traffic laws and respecting "no trespassing" signs when wardriving, warwalking, etc. However, it also warns people "never to connect" to open networks and suggests that wardrivers adopt the "hiker motto" of "take only pictures, leave only footprints," noting that "[d]etecting SSID's[312] and moving on is legal, [but] anything else is irresponsible to yourself and your community."[313] At this point, it is impossible to determine the extent to which the ethic has been adopted, although it was promoted at a worldwide wardrive event.[314]

¶ 105 Did the wardialers and hackers of the 1980s and 1990s have different motivations than the wardrivers of today? Although the security aspects remain the same—recall wardialers also claimed that they were providing a public service by exposing security flaws—wardialers did not benefit from the dialing itself. The wardialers only benefited if they found a computer from which they could download information. Likewise, wardrivers do not benefit if they only record the availability of open networks. In order to benefit, wardrivers must take an additional step and *access* the open networks. Yet there is a key common-sense difference: wardrivers learn where to access the Internet for free, whereas wardialers did not obtain free access from wardialing. Unless wardialers were phreaking or calling locally, they had to pay to dial and gain access. Wardriving costs nothing, and wardrivers gain free Internet access.

[310] *See* Farrow, *supra* note 307.

[311] *See* Renderman, *supra* note 9.

[312] SSID is short for "Service Set Identifier," a 32-character code attached to the header of packets sent over a WAP that has a password character when a device tries to connect to it.

[313] Renderman, s*upra* note 9 (footnote added).

[314] One Internet publication has noted that the periodic "WorldWide WarDrives" refer their users to the Stumbler Code of Ethics. However, citations of the Code are not widespread. *See* Eric Griffith, *Mapping the Lack of Security,* SILICONVALLEY.INTERNET.COM, Oct. 25, 2002, *available at* http://siliconvalley.internet.com/news/article.php/1488541 (describing the WorldWide WarDrive that took place in mid 2002 in multiple global locations and indicating that the group advised the users to abide by the Stumbler Code of Ethics).

¶ 106 Free Internet access is where wardriving's ethical dilemma is most pronounced. As long as the WAP owner has the contractual right to share the Internet connection, no such dilemma arises. Also, normal users often blend in with wardrivers. An individual who opens her notebook in a coffee shop and is given a choice among networks—some free, others subscription—will likely choose one of the free networks. And in many cases it is nearly impossible for the wardriver (or casual Wi-Fi user) to distinguish between (1) open networks that the WAP owner intends to share with others; (2) networks that are only open due to the ignorance of the WAP owner or because of faulty security configurations; and (3) networks that are open because the network operator intends to be open, regardless of whether the network operator has the contractual right to share them. The latter two scenarios introduce profound ethical problems. Both tort and contract law may contribute to a solutions. Each will be briefly explored below.

B. Wi-Fi Manufacturer Ethics

¶ 107 Even the most conservative reading of vulnerability disclosure policies reveals that most software and device manufacturers agree that they have a responsibility to repair serious network vulnerabilities. There have been three "WorldWide WarDrives," and the resulting statistics from 2003 are remarkable: of 88,122 WAPs that were scanned, more than 67% had not enabled WEP security.[315] Furthermore, thousands of articles, websites, and news reports have warned consumers, software manufacturers, and equipment manufacturers that their wireless networks may be unsecured. The press has exposed the serious consequences of network vulnerabilities, including criminal access to central databases where credit cards are stored, distribution of anonymous spam, and downloading child pornography.[316] Wardrivers have sent a clear message to consumers and manufacturers alike: neglect to enable WEP security, and you are vulnerable to attack.

¶ 108 There is no single explanation for why 67% of consumers and manufacturers have chosen to not to enable the built-in security measures on their wireless LANs. Some may wish to share their networks. Others—in spite of the widespread publicity—may not be aware of or understand the security problems associated with their wireless products. A third category might comprise those individuals who lack the expertise to set up the security. Finally, a fourth category includes those (like the author of this article) who are aware of the problems and know how to solve them, but are just too lazy to do it. While most WAPs come with a WEP security feature, that feature must often be configured by accessing the network device directly and configuring its firmware.[317] This extra step is not complicated for the savvy user; however, it does take some time and some troubleshooting effort. The computer industry has grown because it makes easy-to-use products, and users have become accustomed to relying upon assurances by hardware and

[315] *See* WorldWide WarDrive III statistics, *available at* http://www.worldwidewardrive.org/ (last visited June 21, 2004).

[316] See discussion *supra* Section IV.

[317] Firmware is software that is embedded in a hardware device. An example of firmware is a computer program in a read-only memory (ROM) integrated-circuit chip. Most WAPs are controlled by firmware, and patches and updates may be downloaded for free at the company's website.

software makers that these products are safe and secure.[318]

¶ 109 To date, manufacturers have not met their burden in Wi-Fi security. Building on former Presidential Cyber Security Adviser Clarke's suggestion that manufacturers should take responsibility for their actions,[319] recent academic debate has convincingly argued that advanced manufacturers, though in a far better position than consumers to repair security problems, tie consumers to their products through contractual agreements and end up doing nothing about security:

> Vendors, who do or should know better, are careful to enforce the user's illusion [of security] because it increases the sale of their products and services … The user, usually lacking the knowledge to assess their vulnerability to attack, typically accepts the assurances of the vendor or integrator. The vendors usually protect themselves from liability behind blanket disclaimers, which typically make the user assume all liability for failures, even though the user does not have the necessary expertise or information to evaluate the vendor's claims.[320]

¶ 110 Unfortunately, the responsibility for enabling appropriate levels of software security and for any subsequent security issues that arise ends up on the consumer's doorstep. Solving these security problems may involve a long and expensive process, but a solution is not impossible. In fact, interfaces that automate security measures for setting up security as plug-and-play products can be developed, similar to the password protection that exists on web email systems or the passwords that users often put into their own screen savers. While fixing vulnerability problems cannot be accomplished overnight, where it is blindingly clear—as it is here—that consumers are exposed to serious security threats, product manufacturers have an ethical responsibility to eliminate or at least reduce these dangers.

1. Tort Law Remedies Against Manufacturers Yield Unsatisfactory Results

¶ 111 Manufacturers may also be—and perhaps should be—liable in tort for their (in)action (*i.e.,* for leaving the default configuration of wireless devices open and unsecured). Tort claims may be particularly appealing to plaintiffs, since courts rarely award punitive damages in a contract suit.[321] Moreover, some consumers could find their contract claims barred due to warranty disclaimers or have difficulty in proving breach.

¶ 112 Applying tort law to solve an ethical problem, however, is like forcing a square peg into a round hole. In addition to procedural and contractual bars, a consumer is

[318] *See* John R. Michener et al., *"Snake-Oil Security Claims"- The Systematic Misrepresentation of Product Security in the E-commerce Arena*, 9 MICH. TELECOMM. & TECH L. REV. 211, 223 (2003).

[319] Robert Lemos, *Security Czar Points Finger of Blame*, CNET NEWS.COM, July 31, 2002, *available at* http://zdnet.com.com/2100-1105-947409.html (quoting Richard Clarke).

[320] *Id.*

[321] *See, e.g.,* Patrick S. Ryan, *The U.S. Supreme Court Introduces the 'Single Digit Multiplier' to Punitive Damages*, EUR. L. REP. No. 5 (2003) (discussing the recent advances in U.S. punitive damages law after *State Farm v. Campbell*).

unlikely to be able to allege physical injury, which is generally viewed as a requirement for a successful tort claim.[322] Courts have concluded that pure economic loss in tort is not recoverable, because tort cases do not "invade an interest of the plaintiff to which the law of negligence extended its protection."[323] Economic losses are recoverable only when they are accompanied by either personal injury or property damage.[324]

2. Contract Law Remedies Against Manufacturers Yield Better Results, Though Much Progress is Still Needed

¶ 113 Tort law remedies may be extremely problematic, but contract law remedies are also somewhat troublesome. The Uniform Commercial Code (UCC) requires that every contract include, absent an exclusion, an implied warranty that a product is "merchantable" (*i.e.*, it is suitable for the ordinary purposes for which it is used).[325] The contract may also contain a warranty of fitness for a particular purpose. It is implied that the manufacturer has reason to know that the user is relying on its skill or judgment to create or select a product that is fit for the consumer's particular purpose.[326] Absent an exclusion, such knowledge constitutes an implied warranty of fitness for this particular purpose.[327] Implied warranties, however, are relatively easy to exclude from a contract by the use of "expressions like 'as is,' 'with all faults,' or other language which in common understanding calls the buyer's attention to the exclusion of warranties and makes plain that there is no implied warranty."[328] This exclusion, however, must be conspicuous,[329] and courts will enforce the exclusion unless it is "unconscionable."[330] Many technology-related contracts conspicuously disclaim implied warranties.[331] While it is unusual for software contracts between business enterprises to be found unconscionable,[332] at least one jurisdiction has specified a different threshold for consumer purchases.[333]

¶ 114 Conspicuousness and unconscionability are consumers' best weapons against Wi-Fi product manufacturers who sell products with default configurations that leave consumers open to attack. It can probably be assumed that Most Wi-Fi products contain

[322] W. KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 681 (5th ed. 1984).

[323] Duffin v. Idaho Crop Improvement Ass'n, 895 P.2d 1195, 1200 (Idaho 1995) (a state tort case refusing economic damages in negligence).

[324] *Id.*

[325] U.C.C. § 2-314 (2004).

[326] *Id.* at § 2-315.

[327] *Id.*

[328] *Id.* at § 2-316(3)(a).

[329] *Id.* at § 2-316(2).

[330] *Id.* at § 2-302(1).

[331] *But see* Comms. Groups, Inc. v. Warner Comms., Inc., 527 N.Y.S.2d 341, 346, (Civ. Ct. 1988) (noting that "[t]he contractual provision relied on by CGI . . . fails to alert or call to defendant's attention the exclusion of any warranty of merchantability or fitness for a particular known purpose . . . Nor does this clause use the words 'merchantability', 'fitness', 'disclaimer', 'as is', 'warranty' or 'all faults.'").

[332] Toucan Scan, Inc. v. Hell Graphics Sys., Inc., 1993 WL 74891, at *1 (D. Or. 1993).

[333] *See* MD. CODE ANN. § 2-316.1 (2004). "The provisions of § 2-316 (allowing exclusion or modification of warranties) do not apply to sales of consumer goods, as defined by §9-109, services, or both." *Id.*

warranty disclaimers, as do most products in high-technology and software businesses.[334] However, for a manufacturer to properly exclude an implied warranty of merchantability, the disclaimer must conspicuously mention merchantability.[335] Moreover, to exclude or modify the implied warranty of fitness for a particular purpose, the disclaimer must be in writing and conspicuous.[336] In order for a term to be considered "conspicuous," the manufacturer must display it in such a way that a reasonable person against whom the disclaimer will operate should notice it.[337]

¶ 115 In one case, the purported warranty disclaimer was placed on a tag attached to a feed bag under the heading "warranty," but was found to be insufficiently conspicuous.[338] In reaching its decision, the court emphasized the following: (1) there was no contrasting color or particular emphasis on any portion of the asserted disclaimer; (2) the tag was attached among other tags and was not in a "particularly conspicuous location;" (3) the warranty tag was the least conspicuous bit of writing on the bag; and (4) "warranty" suggests that the warranties were included rather than excluded.[339]

¶ 116 Imagine that a consumer installs her Wi-Fi device and, after plugging it in, sees no disclosures of any kind. There are no flashing warning signs (a feature that would be easy to build into plug-and-play products) that inform her that the product that she is installing is open and that it could make her system less secure. To see the disclosure, the consumer has to open a cellophane-sealed booklet. However, the creator could easily include menus that instruct her how to set up the built-in WEP security features. So while it would be amazingly simple to create an electronic flashing disclaimer that puts people on notice, consumers instead have little or no notice that their product is open and exposed. Since nearly all other computer components come with default passwords, it is reasonable for the average consumer to assume that WAPs would as well.

¶ 117 One final analogy drives this point home. The Uniform Computer Information Transactions Act (UCITA) includes implied warranties in software products. Section 405 creates implied warranties in two situations where the consumer relies upon the manufacturer's expertise:[340] (1) when the computer information is fit for the licensee's particular purpose and (2) when the components will fit together as a system. Whether or not these warranties arise is a question of fact determined by the circumstances at the time the contract was created.[341] If one believes—as this article argues—that the products do not fit together as a system when the default configuration creates a security hole in the system, then (at least conceptually) the UCITA supports a consumer claim.

[334] *See* Michener, *supra* note 318, at 220 (assuming a seller will almost always attempt to disclaim implied warranties when entering into a contract).

[335] U.C.C. § 2-316(2). *See also* Eaton v. Magnavox Co., 581 F. Supp 1514 (E.D. Mich., 1984).

[336] *Eaton*, 581 F. Supp. at 1514.

[337] U.C.C. §1-201(b)(10).

[338] Mallory v. Conida Warehouses, 350 N.W.2d 825 (Mich. Ct. App. 1984).

[339] *Id.* at 827.

[340] Uniform Computer Information Transactions Act § 405, comment 1 (2002).

[341] *Id.* at comment 3 (2002).

VIII. CONCLUSION

¶ 118 Wardriving and warchalking represent the newest trends in an evolving phenomenon that has spanned several decades. Indeed, the public has been exposed to many forms of hacking and network access in the past and will continue to see variations of this theme in the future. Although the issue began to gain widespread publicity around the time that the movie *WarGames* was released in 1983, hacking activities were already occurring then and will continue to occur for the foreseeable future. One change is the methods that hackers use to access information. Twenty years ago, back doors were found via dial-up access. Today, they are accessed via the Internet and intranets using either wired or wireless means. As the technology changes, the law and society must alter their perceptions of the issue. As the Puffer case shows, there are still "shoot the messenger" prosecutions; however, such prosecutions will occur less as law enforcement becomes more adept at differentiating between identifying a network vulnerability and exploiting one.

¶ 119 Because hackers have exposed the weaknesses of open WAPs, networks are slowly becoming more secure. Such public-service efforts spur manufacturers to take more responsibility for creating secure plug-and-play WAP products (and other computer interfaces). Manufacturers should undertake a strategy to provide information about their products in order to improve security. Even if manufacturers are not legally obligated to do so, there are compelling ethical motivations for taking such the initiative. In fact, both hackers and manufacturers should intensify their efforts to develop a mutually beneficial approach. Along this vein, manufacturers should continue to develop disclosure mechanisms that clearly notify consumers of the security problems that may exist, as well as possible remedies. Failure to do so will only continue to feed the ethical tensions between white-hat, gray-hat, and black-hat hackers. Furthermore, neglecting to address vulnerability problems head-on will perpetuate the proliferation of derivative hacking activities, such as theft of services, theft of data, and access to child pornography that—unlike wardriving—*do* implicate criminal elements.

¶ 120 To be certain, there is a distinct difference between those who wish to expose vulnerabilities and those who wish to exploit them. These differences have led to a split between hackers, crackers, and phreaks. Hackers have seen their commercial stock rise as they help corporations build firewalls and security measures. Likewise, some crackers and phreaks have been prosecuted for fraud, and criminal hackers now find it much more difficult to evade the authorities. New laws have been passed, including the DMCA, and the increased international cooperation in locating and punishing those who misuse the technology has separated the technology enthusiasts from the criminals.

¶ 121 These changes have caused a new trend to appear: hacker self-regulation through ethical codes of conduct. Hackers have finally begun to step away from anarchistic declarations of unbridled hacking freedom, and they have begun to articulate detailed, codified policies. Although these policies are neither fully developed nor have the parties reached consensus, they are promising. In the future, hackers may self-regulate by a code of ethics in much the same way that other professions do. Evidence shows that hackers now work closely with the corporations against whom they previously battled. Similarly, vulnerability disclosure policies have been proposed by large corporations that are learning the value of working with the hacking community. Hopefully, both trends will continue to evolve and a true hacking code of ethics will emerge.

¶ 122 In the meantime, wardriving is and should remain legal. The underlying problems with unsecured networks and unlocked doors should be fixed, and the neighborhood watchman should not be punished for kindly warning her neighbor that his door is unlocked.