International Journal of Communications Law & Policy

Issue 9 - Special Issue on Cybercrime, Autumn 2004

REAL WORLD PROBLEMS OF VIRTUAL CRIME

By Beryl A. Howell[†]

ABSTRACT

Theoretical debates about how best to address cybercrime have their place, but, in the real world, companies and individuals face harmful new criminal activity that poses unique technical and investigatory challenges. One of the greatest challenges posed by this new technology is how to combat wrongdoing effectively without netting innocent actors. This Article will present three case studies drawn from recent high-profile news stories to illustrate the pitfalls of legislating in the e-crimes arena.

.

Theoretical debates about how best to address cybercrime have their place, but, in the real world, companies and individuals face harmful new criminal activity that poses unique technical and investigatory challenges. There is nothing virtual about the real damage on-line crime can inflict off-line to victims. At the same time, technology is inviting uses that may result in significant, though sometimes inadvertent, criminal and civil liability. The law is not always crystal clear about whether specific conduct is a crime, or about which tools investigators may use to collect evidence identifying the scope of the criminal activity and the perpetrator. In this Article, three stories based on real-life cases are described that highlight murky areas of the law.

At the risk of spoiling the suspense, let me make the moral of these stories plain at the outset: specific laws directed to specific problems are important for two main reasons. First, they serve to guide law enforcement as to how investigations may be conducted with appropriate respect for civil liberties and privacy. Second, specific laws make clear to people the boundary of legally permissible conduct.

Does this require endless effort to update the laws to keep pace with technology? Yes, but Congress returns every year with the job of making new laws. Will the pace of legal changes always be behind technological developments? Yes, but in my view the correct pace is a slow one. By the time a proposal has gone through the legislative process, the problem it seeks to address will have become more defined. Policy-makers

[†] Managing Director and General Counsel of the Washington, D.C. office of Stroz Friedberg, LLC, a technical services and professional consulting firm specializing in digital forensics and cybersecurity investigations. She previously served as the General Counsel on the U.S. Senate Judiciary Committee for Senator Patrick J. Leahy (D-VT). Shorter versions of this paper were presented orally at the Yale Law School Conference on Cybercrime and Digital Law Enforcement, "Digital Cops in Virtual Environment," on March 27, 2004, and published as *Ambiguities in U.S. Law for Investigators*, 1 DIGITAL INVESTIGATION 106-11 (2004). Many thanks to Donald E. Allison and Aaron Stanley of Stroz Friedberg, LLC for their contributions to both the investigations discussed in this article and for their editing contributions.

.

are better able to craft a narrow and circumscribed law to address a clearly defined problem, and thus minimize the risk of an overly expansive law that could chill innovation and technological development.

I. THE CASE OF THE SNOOPING STAFFERS AND PEEKING POLITICOS:

When does snooping cross the legal line of computer abuse?

The first case-study arises from a computer investigation recently conducted within the Committee on the Judiciary of the United States Senate. The facts of this case are quite simple. In November 2003, conservative newspapers and a website – the *Wall Street Journal* editorial page, the *Washington Times*, and the Coalition for a Fair Judiciary – published excerpts from approximately 19 internal staff memoranda to Democratic Members of the Senate Judiciary Committee.[1] As is frequently the case with instances of computer security breaches, the scope of the breach is usually far more serious than the initial problem suggests. Indeed, these nineteen leaked memoranda were just the tip of the iceberg.

The Senate Sergeant of Arms conducted a limited "administrative, fact-finding inquiry" at the bipartisan request of the Chairman of the Judiciary Committee and Senior Democratic Members into the circumstances surrounding the theft of the Democratic staff memoranda.[2] The report of the inquiry (the "Pickle Report") revealed that a staffer for Senator Hatch and a staffer for Majority Leader Frist had, on a daily basis for almost 18 months, methodically accessed files of targeted Democratic staffers working on judicial nominations, taking almost 4,700 documents in the process.[3] Evidence was uncovered that the Hatch and Frist staffers took steps to cover their tracks and conceal their theft of the Democratic staff memoranda, including keeping the stolen documents in a zipped, *i.e.* compressed, password-protected folder on the Hatch staffer's computer.[4]

The Committee file server was shared by both Democrats and Republicans, with each staffer having his or her own account, associated with a personal electronic folder for storage of documents or other data. Staff working for the same Senator had permission to share certain files among themselves, but no other Members' staffs were permitted to see these files.[5] At least that is how the permissions had worked, were understood to work, and were supposed to work. However, when a new systems administrator had been hired in 2001, he did not set the permissions protocol correctly for

[1] *See, e.g.*, *Review & Outlook*, WALL ST. J., Nov. 14, 2003, at A12; *The Case Was Fixed*, WASH. TIMES, Nov. 18, 2003, at A01; Press Release, The Committee for Justice, Fact Sheet: The Democratic Judicial Memo Investigation (Jan. 22, 2004), *at* http://committeeforjustice.org/cgi-data/press/files/10.shtml (last visited Nov. 9, 2004).

[2] SERGEANT OF ARMS U.S. SENATE, 108TH CONG., REPORT ON THE INVESTIGATION INTO IMPROPER ACCESS TO THE SENATE JUDICIARY COMMITTEE'S COMPUTER SYSTEM, at 7 (2004) [hereinafter "Pickle Report"]. The inquiry was necessarily limited since the Sergeant of Arms has no subpoena powers.

[3] *Id*. at 9.

[4] *Id*. at 8.

[5] *Id*. at 18.

over half of the staff on the Committee, so the files in those accounts were accessible to any user with access to the server.[6]

One might think the discovery that Republican staffers were snooping through the internal and confidential memoranda among Democratic staff and Members would have the effect of throwing gas on an already simmering partisan fire. Interestingly, that is not what happened. Instead, virtually every Committee Member from both sides of the aisle agreed that this spying was an appalling breach of both confidentiality and custom.

There has been public debate, however, about whether a crime had been committed, which is somewhat ironic since this incident involved the Committee responsible for crafting the original Computer Fraud and Abuse Act ("CFAA") as well as every amendment to that law for the past decade. [7] Was the unauthorized access by the Republican staffers simply immoral or was it a crime?

Former White House Counsel C. Boyden Gray, the Chairman of the Committee for Justice, former Majority Leader Trent Lott, and others have asserted that no crime was committed since the improperly configured security settings on the Committee file server provided easy access.[8] The Committee for Justice promulgated a "fact sheet" asserting that no crime occurred because there was no "hacking."[9]

Yet, by its plain terms, the CFAA prohibits both unauthorized access, which is colloquially called "hacking," and exceeding authorized access of "protected computers."[10] "Hacking" is not a defined term, nor even used in the law. "Unauthorized access" is also not defined in the law, while the phrase "exceeds authorized access" is

---

[6] *Id*. at 11.

[7] 18 U.S.C. § 1030 (2004).

[8] Letter to the Editor from C. Boyden Gray, Chairman of Committee for Justice, Faulty Judiciary Network: Let's Establish the Facts (Dec. 23, 2003) *in* WALL ST. J., Dec. 23, 2003, at A15 (quoting Mr. Gray as stating, "The Democrats designed a faulty 'shared network' where files could be accessed freely by staffers of either party; if you had material you wanted kept completely confidential, you were advised to store it on your own hard drive. No one exceeds their authority when they log on and access files on their own computer's desktop. Democrats, in other words, were the ones who disclosed their own documents, which were in fact entirely unrestricted."). *See also* Charlie Savage, *GOP Downplays Reading of Memos*, BOSTON GLOBE, Jan. 23, 2004, at A3, *available at* http://www.boston.com/news/nation/articles/2004/01/23/gop_downplays_reading_of_memos/ (last visited Nov. 9, 2004); Alexander Bolton, *Leak Staffer Ousted; Frist Aide Forced Out in an Effort to Assuage Dems*, THE HILL, Feb. 5, 2004, *available at* http://www.hillnews.com/news/020504/leak.aspx (quoting Senator Trent Lott (R-Miss.) as stating, "[r]ight now I think that was pretty unfair . . . I don't have the impression he did anything wrong . . . I don't know the details, but I would not be a friend in firing a highly qualified staffer") (last visited Nov. 9, 2004); Geoff Earle, *Leak Probe Expands; Santorum Assails Signs Investigation Targets GOP Aides*, THE HILL, Feb. 11, 2004, *available at* http://www/hillnews.com/news/021104/probe.aspx (quoting Senator Santorum as stating, "[i]f there's anything criminal, it's the behavior of the Democrats") (last visited Nov. 9 2004); Dahlia Lithwick, *Memogate*, SLATE .COM, Feb. 19, 2004, *at* http://www.slate.com/id/2095770 (reporting "some conservative groups claim that no crime occurred.") (last visited Nov. 9, 2004).

[9] The Committee for Justice, *supra* note 1 (regarding the appropriateness of the Sergeant of Arms' investigation, "It was a mistake to give credence to the Democrat complaint that any impropriety had occurred with regard to the disclosure of these documents to the press . . . if Senate computers were hacked into, a law might have been violated . . . Was there a 'hacking'? No, it appears not . . . the documents in question were inadvertently disclosed and obtained off an unsecured shared network accessible to both Democrat and Republican Judiciary Committee staff . . . In short, there was no breaking and entering. Staffers were entitled to access their own desktop computers and the committee network on which the documents were inadvertently disclosed.")

[10] *See* 18 U.S.C. § 1030(e)(2) (2004).

broadly defined to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[11] The CFAA contains absolutely no requirement that data be secured and rendered inaccessible to unauthorized users to enjoy the protection of the statute.[12] On the contrary, this statute imposes misdemeanor criminal liability for merely obtaining information stored on a computer system by accessing a computer without authorization or by exceeding authorized access.[13]

The shrill partisanship voiced both by some Senators who do not serve on the Judiciary Committee, and by outside groups, obscured the fairly simple legal questions posed in the Peeking Politicos debacle: (1) did the surreptitious accessing, reading, and copying of Democratic staff memoranda on multiple occasions over a period of months by Republican staff constitute "obtaining information" within the meaning of the CFAA; (2) did this activity by Senator Hatch's staffer, who was authorized to use the Senate Judiciary server, fall within the CFAA's prohibition of exceeding authorized access; and (3) did directions by Majority Leader Frist's staffer to Senator Hatch's staffer to engage in this activity run afoul of the CFAA's prohibition on unauthorized access?

The plain terms of the statute appear to provide affirmative responses to these questions, a conclusion corroborated by explanations of the intended scope of the law found in the legislative history. Over the last twenty years, the CFAA has undergone several significant amendments that have expanded the law's range from covering only government and financial institution computers to covering virtually every computer connected to the Internet. Further, there has been added a civil cause of action as an enforcement mechanism to supplement the criminal penalties for significant breaches. As originally enacted in 1984, the CFAA penalized: (1) knowingly obtaining classified information,[14] financial records, or credit histories in financial institutions;[15] (2) using, altering, or destroying any government information[16] by accessing a computer without authorization; and (3) "having accessed a computer with authorization, us[ing] the opportunity such access provided for purposes to which such authorization does not extend."[17]

---

[11] 18 U.S.C. § 1030(e)(6) (2004).

[12] The Computer Fraud and Abuse statute, in pertinent part, bars (1) intentionally accessing a computer; (2) to obtain information from "any department or agency of the United States," which is defined at 18 U.S.C. § 1030(e)(7) to include "the legislative or judicial branches of the Government"; (3) "without authorization" or by "exceeding authorized access," which is defined at 18 U.S.C. § 1030(e)(6) to mean accessing a computer with authorization but to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter.

[13] 18 U.S.C. §1030(c)(2)(A). This illegal activity may also be a felony offense with up to 5 years imprisonment if committed for commercial advantage, private financial gain, in furtherance of any criminal or tortuous act, or if the value of the information exceeded $5,000.

[14] 18 U.S.C. § 1030(a)(1) (1984) (enacted as part of the Comprehensive Crime Control Act of 1984, P.L. 98-473, 1984).

[15] *Id.* at (a)(2).

[16] *Id.* at (a)(3) (penalizing "Whoever . . . knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation.").

[17] *Id.* at (a)(1)-(3).

The conduct prohibited by "unauthorized access" is "analogous to that of 'breaking and entering'."[18] By contrast, the conduct barred by exceeding authorized access was intended "to make it a criminal offense for anyone who has been authorized to use a computer to access it knowing the access is for a purpose not contemplated by the authorization. As a result, it prohibits access to a computer to obtain the described data when the perpetrator knows that the access is not authorized or that it is not within the scope of a previous authorization."[19] On the other hand, information obtained only incidentally, "pursuant to an express or implied authorization," or in accordance with "normal and customary business procedures and information usage" is not covered.[20]

The cumbersome phrase used in the original CFAA — "having accessed a computer with authorization, uses the opportunity such access provided for purposes to which such authorization does not extend" — was condensed to the current language of "exceeds unauthorized access" in order "merely to clarify the language in existing law"[21] and "simplify the language."[22] Inadvertent or mistaken access to computer files which a person is not authorized to view does not run afoul of the law. The Senate Judiciary Committee acknowledged that distinguishing "between conduct that is completely inadvertent and conduct that is initially inadvertent but later becomes an intentional crime" may be "a difficult line to draw in the area of computer technology because of the possibility of mistakenly accessing another's computer files."[23] Yet, both the House and Senate Judiciary Committees authorizing this criminal statute made clear that exploiting access that was unauthorized would not be excused, even if the initial discovery of the means to such access was inadvertent or accidental. The Senate Judiciary Committee explained:

---

[18] COUNTERFEIT ACCESS DEVICE AND COMPUTER FRAUD AND ABUSE ACT OF 1984, H.R. REP. NO. 98-894, at 21 (1984) *reprinted in* 1984 U.S.C.C.A.N. 3182 [hereinafter *1984 House Judiciary Report*].

[19] *Id*.

[20] *Id*.

[21] COMPUTER FRAUD AND ABUSE ACT OF 1986, H.R. REP. NO. 99-612, at 11, (1986) [hereinafter *1986 House Judiciary Report*].

[22] COMPUTER FRAUD AND ABUSE ACT OF 1986, S.R. REP. NO 99-432, at 9 (1986) [hereinafter *1986 Senate Judiciary Report*). The CFAA was first significantly amended by the next Congress after its initial passage, including by (1) changing the scienter requirement from "knowingly" to "intentionally" for the prohibitions in sections (a)(2) and (3) to make amply clear that only intentional acts were covered and not "mistaken, inadvertent or careless ones," *id.* at 5; (2) removing from the prohibition in section (a)(3), which bars unauthorized access to government computers, coverage of insiders in order to protect whistleblowers and leaving intradepartmental trespass to be handled by other applicable laws, *id*. at 7-8, 20-23 (additional views of Messrs. Mathias and Leahy); and (3) adding three new offenses in new subsections (a)(4), (5) and (6). While subsection (a)(3) continues only to apply to outside hackers, subsection (a)(2), which bars both outsiders and insiders from unauthorized access to "protected computers" to obtain information, was amended in 1996 by the National Information Infrastructure Protection Act, S. 982, sponsored by Senators Kyl, Leahy and Grassley, to cover federal government computers within the definition of "protected computer." The purpose of this amendment was to increase privacy protection for information stored on government computers in the wake of public and congressional reports on "[g]overnment employees who abuse their computer access privileges by snooping through confidential tax returns, or selling confidential criminal history information from the National Crime Information Center." 142 CONG. REC. S10889 (daily ed. Sept. 18, 1996) (statement of Sen. Leahy).

[23] *Id.* at 14.

> [T]he Committee would expect one whose access to another's computer files or data was truly mistaken to withdraw immediately from such access. If he does not and instead deliberately maintains unauthorized access after a non-intentional initial contact, then the Committee believes prosecution is warranted. The individual's intent may have been formed after his initial, inadvertent access. But his is an intentional crime nonetheless, and the Committee does not wish to preclude prosecution in such instances.[24]

The conduct covered by the term "obtaining information" has been consistently interpreted to include "mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of [18 U.S.C. § 1030(a)(2)]."[25]

The plain terms of the CFAA, as informed by the legislative history, supports the following analysis of the Peeking Politicos activity: As the Pickle Report noted, the "practice in the Judiciary Committee is to 'share' certain files among staff working for the same Senator."[26] Each user also "should have exclusive access to his or her own directory."[27] In short, a Committee staffer is authorized to access his or her personal folder as well as shared files archived or stored on the server by staff employed by the same Member for whom that staffer is employed. This authorization is limited and does not cover access to, let alone the copying or transfer within or without the Senate, of private, confidential information from the archived files of Senators'offices. The latter activities would exceed any such limited authorized access to the Committee server and would likely constitute a misdemeanor violation of section 1030(a)(2) of the CFAA.

Moreover, directions or requests by a staffer with no authority to a staffer with limited authority to exceed that limited authority for purposes of obtaining data on a Committee server, as the Pickle Report indicated that the Majority Leader's staffer did, may rise to the level of aiding and abetting a violation, or itself constitute obtaining unauthorized access. The prohibition on unauthorized access to federal government computers does not only apply to persons entirely outside the government. On the contrary, the Committees authoring the CFAA explained:

> The Committee does not intend to preclude prosecution under this subsection if, for example, a Labor Department employee authorized to use Labor's computers accesses without authorization an FBI computer. An employee who uses his department's computer and, without

---

[24] *Id.*; *see also 1986 House Judiciary Report*, at 10 ("The Committee does not intend to prevent prosecution of a person under this subsection whose initial access was inadvertent but who then deliberatively maintains access after a non-intentional initial contact").

[25] *1986 Senate Judiciary Report*, at 6-7; *see also 1986 House Judiciary Report*, at 10 ("There was some concern evidenced ... by the Department of Justice and others that the term 'obtains information' . . . makes this subsection something other than an unauthorized access offense. The Committee disagreed with this interpretation. THE NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1995, S.R. NO. 104-357, at 7 (1996) [hereinafter *1996 Senate Judiciary Report*] (highlighting that as used in subsection 1030(a)(2), "the term 'obtaining information' includes merely reading it. There is no requirement that the information be copied or transported. This is critically important because, in an electronic environment, information can be 'stolen without asportation, and the original usually remains intact").

[26] Pickle Report, *supra* note 2, at 18.

[27] *Id.*

> authorization, forages into data belonging to another department, is engaged in conduct directly analogous to an 'outsider' tampering with Government computers. In both cases, the user is wholly lacking in authority to access or use that department's computer. The Committee believes criminal prosecution should be available in such cases.[28]

In addition to facing a possible misdemeanor violation, the activity of the Peeking Politicos may have potential civil liability repercussions as well. The CFAA authorizes civil actions for compensatory damages or injunctive relief by any person who suffers (1) any "damage," which is defined to mean any impairment to the integrity or availability of data,[29] or (2) any "loss," which is defined to mean any reasonable cost of responding to an offense, conducting a damage assessment and restoring data, any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[30] The staffers who obtained unauthorized access to the Democratic staff memoranda may be subject to civil suit for damages, for example, by the Senate, which has incurred expenses in the investigation into what happened, including the costs both of personnel diverted from other duties in the office of the Sergeant of Arms to focus on the investigation, and of consultants hired to conduct forensic examinations of the systems involved.

The scope of the activity covered by the terms "access without authorization" and "exceeds authorized access" ranges from simple snooping by authorized users of a network, such as employees inappropriately accessing confidential personnel files of other employees or students accessing or altering grades, to seriously damaging activity, such as the theft of trade secrets or other confidential information. This leaves enormous discretion to prosecutors. In a politically charged matter, such broad discretion may be both unwelcome and uncomfortable. One commentator recently noted

> [i]f it is widely believed that some conduct may technically fall within the language of the CFAA but should in fact not be criminal, the law should be amended. Reliance on the 'reasonable exercise' of prosecutorial discretion is not an adequate response. The text of the statute should reflect such limits.[31]

The Pickle Report stopped short of making any recommendations for the referral of individuals for criminal violations, but did outline the relevant elements of potentially

---

[28] *1986 Senate Judiciary Report*, at 8.; *see also 1986 House Judiciary Report*, at 11 ("The Committee does not intend to exclude under 1030(a)(3) conduct by a Federal employee who is an authorized user, for example, of a Department of Labor computer but without authority accesses a Department of Defense computer while at work or in a similar fashion using his own personal computer at home to access without authority a Department of Justice computer system").

[29] 18 U.S.C. § 1030 (e)(8) (2004).

[30] 18 U.S.C. § 1030(g) and (e)(11). Notably, the CFAA requires proof of more elements for civil liability than for criminal liability. The same conduct that may constitute a misdemeanor criminal charge may not support civil liability, which requires the plaintiff to show damage to the availability of data or financial loss.

[31] Cybercrime Posting by Joseph Metcalfe, Associate Professor at the University of Oregon School of Law (March 22, 2004) *at* http://hermes.circ.gwu.edu/cgi-bin/wa?A2=ind0403&L=cybercrime&F=&S=&P=70 (last visited Nov. 10, 2004).

applicable criminal offenses.[32] A bipartisan group of Members referred the matter to the Justice Department, which in turn, assigned the investigation to the U.S. Attorney for the Southern District of New York.[33] The ending to this story must await the prosecutors' decision as to whether a crime was committed.

II. THE CASE OF THE PARENTAL NIGHTMARE

When does file-sharing cross the legal line of child porn distribution?

In some situations, there may be no question that the computer activity at issue is a crime, but the technology creates issues about whether the crime was committed by the computer user or the computer program.

This story starts one morning a few months ago, when a suburban Mom's morning coffee was interrupted by a knock at the door. It was FBI agents announcing they were there to question, and possibly arrest, the child pornography distributor living and using a computer in the house. They determined the computer being used to distribute child porn – a felony to possess and to distribute – was in the teenage son's room. Like over 60 million other people,[34] he had installed KaZaa on his computer. The teenager had then gone searching for erotic material, which he downloaded in his shared KaZaa folder. Included in this material were child porn images, which many other Kazaa users then located and downloaded from his home computer.

In fact, unbeknownst to the teenager, his machine had been turned into a supernode on the system. He was unaware of the option buried in the software to prevent this from happening and did not change the default settings, which permitted it. So his machine was being used by many clients and other supernodes to point to files available for sharing, including child porn. The teenager technically did not have all of the child porn files on his computer – which would have been enough for a felony – but he had an index pointing to other locations with child porn. This also made his machine a much bigger target for law enforcement looking for online child porn distributors.

Peer-to-peer (P2P) file sharing programs make distribution a passive act, but no less subject to criminal liability. Many users of P2P programs do not fully realize that the simple act of selecting files or folders to share on KaZaa makes them a distributor of all those files, and that the act of distribution, even if initiated by other users, carries with it hefty criminal and civil liability under criminal copyright laws, child porn laws, and laws restricting the distribution of obscene materials to minors.[35]

This was just the beginning of the parents' problems. They then wanted to find out exactly what the evidence was on their son's computer. Was he actively sending child porn as e-mail attachments to others? Was he merely viewing child porn images online, or was he intentionally storing those images on his computer? Was he actively posting or

[32] Pickle Report, *supra* note 2, at 13, 59-62.
[33] Alexander Bolton, *Miranda Sues Ashcroft: Former GOP Aide Strikes Back Over Memogate Scandal*, THE HILL, Sept. 14, 2004, *available at* http://www.hillnews.com/news/09142004/miranda.aspx (last visited Nov. 10, 2004).
[34] SHARMAN NETWORKS, Business Opportunities, *at* http://www.sharmannetworks.com/content/view/full/55 (last visited Nov. 10, 2004).
[35] 18 U.S.C. § 1470 (2004).

uploading child porn images to any sites? Or was he merely a passive distributor by virtue of having downloaded the illegal images into a KaZaa shared folder, with the program enabling other users to activate the distribution? The answers to these questions could provide a more complete picture of the nature of the teenager's computer activity and a context for the activity involving the illegal child porn images that could be helpful in the defense of their son and to persuade a prosecutor not to charge him. Finding those answers required the analytical services of a computer forensic examiner.

The child porn possession crime is so strict, however, that forensic examiners and even attorneys have to be careful not to have such images in their possession. The law treats child porn essentially like heroin – mere possession, even on behalf of a client to assist in an investigation or defense – is no exception to the crime.[36] As one court put it: "Child pornography is illegal contraband."[37] Special protocols have to be followed for forensic examiners to handle matters involving child porn. These protocols may, in appropriate circumstances, be negotiated with the investigating law enforcement agency and may require specific direction from the court.[38] Stringent controls may be placed on the computer forensic examiner, whichwhich limit the location where the examination takes place, the extent of any copying of the images and the removal of any work product resulting from the examination.

Significantly, even if a forensic examination of a computer reveals that child porn images were not manually downloaded or saved but, as a result of the computer user viewing the images online or receiving pop-up advertising with the images, were stored only in a temporary internet file on the computer, the user may face criminal liability for possession. Images searched out, found and viewed on web pages are automatically saved by the computer's web browser in a browser cache file and stored on the hard drive, until the contents of that file are deleted by the user. Courts have upheld convictions for possession of child pornography for viewing illegal images accessed online, without any manual downloading or saving of the images onto the computer.[39]

---

[36] 18 U.S.C. § 2252(a)(5)(B), bars possession of any child porn, with punishment up to 5 years' imprisonment. The law provides an affirmative defense if the defendant (1) has fewer than 3 child porn images, *and* (2) took prompt steps, without retaining or allowing any person other than a law enforcement agency to access the image, to destroy each image or report the matter, and allow access, to law enforcement.

[37] U.S. v. Kimbrough, 69 F.3d 723, 731 (5th Cir. 1995).

[38] *Id.* at 731 (government refused to allow defendant to copy charged images of child pornography and defense expert was allowed to examine the child porn at the offices of the Customs Service, U.S. Attorney's office or defense counsel's office); Rogers v. State, 113 S.W. 3d 452, 458-59 (Tex. App., 2003) (despite state court direction that defense expert be given access to and allowed to prepare a cloned copy of the defendant's hard drive in a child pornography possession prosecution, the local federal prosecutor advised defense counsel that "obtaining and retaining the mirror image would be grounds for federal prosecution because federal law did not contain an exception for discovery in criminal cases;" defense expert conducted examination in sheriff's office); Glenn Puit, *Arrest Threat: Child Porn Copies Lead to Conflict*, LAS VEGAS REVIEW-JOURNAL, July 28, 2003 (local prosecutor threatened to arrest defense counsel for possession of child porn images even though judge had previously authorized counsel to possess the images in order to assist his client's defense).

[39] United States v. Tucker, 305 F.3d 1193, 1198 (10th Cir. 2002), *cert. denied*, 537 U.S. 1123 (2003) (conviction upheld for possession of files automatically stored in a browser cache because defendant's "habit of manually deleting images from the cache files established that eh exercised control over them"); Commonwealth v. Simone, 2003 Va. Cir. LEXIS 215 (Va. Cir. Ct.) (child porn images recovered from

While we still do not know the end of the story of the Peeking Politicos, the story of the Parental Nightmare ended happily, since the prosecutor declined to prosecute the juvenile. The forensic examination of the teenager's computer confirmed that he did not actively distribute the child porn images, which were nevertheless accessed and uploaded by other KaZaa users.

Changes are already developing in P2P networks to get around the liability risks of possessing and distributing illegal material. One such system involves encrypting the files that a user wants to share, pushing the encrypted files onto an another client machine, and then making the decryption key available at web sites only accessible to Freenet users, along with pointers to where the material may be found.[40] The keys are distributed, not the material, and the person in possession of the encrypted material has deniability about what the subject matter of the encrypted file is. Some in law enforcement are already anticipating a need for new laws to make it illegal to possess a deliberately stored decryption key that the user knows relates to an illegal file.[41]

P2P networks actually make the work of investigators easier, since who is sharing illegal files and how much distribution is occurring may be tracked.[42] In the digital world, users of P2P networks may find that the technology has taken them for a ride across legal lines imposed by strict liability laws for possession and distribution of certain materials, including child porn and infringing copyrighted works.[43]

III. THE CASE OF THE WIFI SPOOFER

When does self-help cross the legal line of unauthorized access?

The opportunities presented by wireless technologies for individuals to conceal the origin of communications may make finding perpetrators of computer crime more difficult, as demonstrated by this final story. For about two years, a company was the target of embarrassing e-mails containing derogatory and sexually explicit patents as attachments. These e-mails were not sent to the company, but worse, sent to the company's clients with spoofed (*i.e.*, faked) e-mail addresses to make the e-mails appear to have come from senior executives within the company. The company's clients did not like receiving these disturbing spoofed e-mails, particularly when the company appeared to be incapable of stopping them, and some clients took their business elsewhere.

---

temporary Internet file on defendant's computer after he viewed but did not manually save images sufficient for conviction since he reached out for and controlled the images at issue); *but see* United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002) ("one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image"); United States v. Perez, 247 F. Supp. 2d 459, 484 n.12 (S.D.N.Y. 2003) (court raised without resolving "the issue of whether images viewed on the Internet and automatically stored in a browser's temporary file cache are knowingly 'possessed' or 'received'").

[40] Geoff Fellows, *Peer-to-Peer Networking Issues — An Overview*, 1 DIGITAL INVESTIGATION 3-6 (2004).

[41] *Id.*, at 6.

[42] *Id.*, at 4 ("the structure of peer-to-peer networks presents opportunities to law enforcement for proactive investigation … This results . . . in prosecutions not for the mere possession of obscene images but rather for distribution , a much more serious offense.")

[43] While criminal copyright liability requires a "willful" intent, civil infringement liability is strict.

The e-mail header information on the e-mails showed the originating IP addresses, which the FBI attempted to trace. The traces, however, did not lead back to the perpetrator, but to random home users' wireless access points to which the perpetrator had gained access. This access was gained by a practice known as "war driving." The perpetrator would drive his car around residential neighborhoods with a laptop equipped with a WIFI card and antenna, searching for unprotected wireless access points to which he could connect. A typical home wireless access point will transmit its signal several hundred feet, well beyond the home's walls. By the time the FBI was able to obtain the subscriber information and location of the WIFI point used by the perpetrator, the perpetrator was, of course, long gone. Wireless access point equipment is sold with no security features enabled to block unauthorized access as the default setting. Many users do not bother, do not wish, or do not know how, to change the default settings on the equipment to block such unauthorized access. This equipment also has the capability to maintain a log identifying the MAC address of every computer accessing the Internet through the WIFI point, but again this log must be activated by the user. Even when access points that the perpetrator co-opted were examined, there were no logs of his particular computer having connected to them. This provided a perfect method for the perpetrator to ensure the anonymity of his e-mail messages.

In addition to war driving, this perpetrator also sent spoofed e-mails from computer labs at various universities in the D.C. area, using false or stolen student accounts, also making him difficult to trace. He used the hijacked student accounts to access a proxy server to conceal the originating IP address of the computer he was using within the University computer lab, and used that proxy server to access e-mail accounts, to which he had obtained unauthorized access at AOL and Yahoo, from which he sent spoofed e-mails.

Almost two years into this expensive harassment, the company turned to my firm for assistance. At that point, the company did not know whether the WIFI Spoofer was one person or a group, a malicious insider or outsider, what the person/persons wanted or what was motivating the harassment. Most of all, the company wanted the damaging e-mail campaign to stop.

Extensive computer forensic analysis of the company's computers and systems helped to rule out a malicious insider as the perpetrator of the e-mail campaign. This analysis revealed, however, a number of unauthorized logins to the company's server over a four-month period in 2003 with originating IP addresses used at a local university. Steps were taken to lock down the security of the company's network.

Sometimes technology has to take a back seat to good old gumshoe work. Through a combination of interviews with people in the industry, including competitors of the targeted company, and government agency personnel involved in patent file production, plus use of a clinical psychologist with expertise in developing detailed profiles based upon text and e-mails, a primary suspect was identified within several weeks.

Over the course of the investigation, we discovered that senior executives at a sister company of the targeted company had received e-mails from a person complaining about the targeted company. Textual and psychological analysis by the clinical psychologist demonstrated that the author of the spoofed e-mails was the same author sending the complaining e-mails (under a fake name) to the sister company. The

psychologist further determined that a single author, not a group, was involved. But who was this person and how were we going to determine whether it was the person identified as the primary suspect?

We sent the complainer an e-mail to see if he would re-engage in communications with representatives of the sister company. In order to find out the IP address of the computer where the email was opened, a technical tool, called a web bug, was used to capture the IP address of the computer where the e-mail was opened.[44] In addition, this tool provides related information about when the perpetrator opened the e-mail, how long the e-mail was kept open, and how long it took the perpetrator to respond after opening the e-mail. This information is relevant to building a profile of the perpetrator and anticipating how to interact with him in an effective manner to identify him.

Web bugs such as the one used in this case capture information generated by the computer system itself, not content that is generated by the computer user. The CFAA was intended to protect the privacy and security of computer content and therefore does not cover computer system information, such as IP addresses. Yet, absent a definition of "information" in the statute, the blurry lines in the scope of the CFAA's coverage of such computer-generated system information must be navigated by aggressive investigators and clients in crisis, who are choosing the technical tools necessary to investigate cybercrime.

After a carefully calibrated series of exchanges, the WIFI Spoofer sent a multi-million dollar extortion demand threatening to unleash a denial of service attack that would be made to appear to come from the targeted company and that would use as a "payload" confidential information on the company and its clients that he had obtained

[44] An IP address is the unique address assigned to every machine on the Internet and consists of four numbers separated by dots. A web bug, or pixel tag, is embedded in an HTML-formatted e-mail message sent to the perpetrator. When the e-mail message is opened, the image tag refers the user's browser to a 1x1 pixel transparent picture stored on a web server under the control of the party embedding the image tag. The web server then keeps a log of all requests for that image and logs the IP address of the browsing host, the time and date of the request and also, in these cases, a referring URL that shows the last URL loaded by the browser so that we can track what site referred the browser to the web server. This type of image tag works similarly to the default logging of a web server, *i.e.,* when a user visits a web site, the web site collects information on the IP address of the visitor's web browser and the date and time when the visit occurred. This type of logging is widely used by web sites to track web page activity for security purposes. Just as a web site tracks the IP address of browsers accessing the web site, the web bug tracks the IP address of browsers on computers where the tagged e-mail message is opened and provides information on when the person opens the e-mail message, the IP address of the browser used to open the email and what type of browser was used (*e.g.*, Microsoft's Internet Explorer, Netscape or Mozilla). It is less intrusive than a cookie, which web sites place directly on a visitor's hard drive and may be used to monitor web surfing activities of a user and to capture personally identifiable data about unsuspecting computer users. Such use of cookies has been found to raise viable claims of violations of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701, though not of the CFAA. *See In re* Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003) (finding defendants' use of web bugs that collected personal information about web site visitors by planting cookies on the visitors' computer hard drives was not violation of ECPA was reversed but district court judgment of no CFAA violation was not disturbed); *In re* Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001) (plaintiff computer users who visited website, www.quicken.com, and had cookies surreptitiously embedded on their hard drives in order to track and record a particular user's movements across the web failed to show allege any economic damage as required under 18 U.S.C. § 1030(g) and that claim was dismissed, but claims under the ECPA survived motion to dismiss).

through "dumpster diving" of the company's trash bins. The perpetrator revealed many additional details that were consistent with the information on the primary suspect we had already identified. At the same time, the primary suspect was put under surveillance, which resulted in placing him in the same place – at a university computer lab – where certain incriminating e-mails originated.

The FBI then arrested him. When the defendant's house in Maryland was searched they found not only computers and other items related to the attempted extortion, but also firearms, components for hand grenades, and the formula and items necessary for making ricin, a deadly toxin. He was detained pending trial, pleaded guilty, and was recently sentenced to 63 months' imprisonment in October, 2004, for violating the CFAA provision prohibiting online extortion. Often in cybersecurity investigations, the threats that the victims are aware of usually are just the tip of the iceberg.

The story of the WIFI Spoofer had a happy ending, at least from the perspective of the victimized company. After almost two years of suffering the repercussions fromof the spoofed e-mail campaign, it took the concerted investigative effort of the FBI, the U.S. Attorney's office and a private cybersecurity firm to track this perpetrator, through use of technical tools, physical surveillance, a clinical psychologist and good interviewing techniques.

This story also points out how the CFAA may stymie legitimate self-help efforts to identify perpetrators of harmful online crimes, and brings full circle the question of the scope of this statute. From the perspective of the Peeking Politicos in the case of the Senate Judiciary Committee server spying case, and of the investigators in the case of the WIFI Spoofer, the reach of the CFAA was a puzzle. This should be a cautionary note in future policy debates over topics such as "spyware." Care must be taken to ensure that legitimate efforts to trace illegal activity by others are not impaired by regulatory measures written so broadly and without clear malicious intent requirements that they suffer from the same scope questions raised by the CFAA.

IV. CONCLUSION

Rapid technological developments in communications technologies are providing new opportunities for violators to cover their tracks, new techniques for investigators to pursue them, and new traps of liability for the reckless computer user. Tensions are inevitable as these developments test the reach of current laws and the circumstances in which putative defendants may find themselves liable and victims may engage in self-help without themselves crossing ill-defined legal lines. It would be ironic indeed if the concern over harmful online activity results in over-regulation of the use of certain technologies with the effect of hamstringing victims and investigators from using those or similar tools to stop or prevent the harmful conduct.