

## REAL WORLD PROBLEMS OF VIRTUAL CRIME

By Beryl A. Howell<sup>1</sup>

Theoretical debates about how best to address cybercrime have their place but, in the real world, companies and individuals are facing new harmful 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 and about which tools investigators may use to collect evidence identifying the scope of the criminal activity and the perpetrator. In this essay, three stories based on real-life cases are described that highlight gaps in 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, both as guidance to law enforcement on how investigations may be conducted, with appropriate safeguards for civil liberties and privacy, and to alert people where legal lines are drawn as a caution against crossing them.

Does this require endless effort to update the laws to keep pace with technology? Yes, but the 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 “go slow” one. By the time a proposal has gone through the legislative process, the problem it seeks to address will have ripened into better definition. The better defined a problem is, the better policy-makers are able to craft a narrow and circumscribed law to address the problem, while minimizing the risk of over-breadth that could chill innovation and technological development.

The first story arises from a computer investigation that has been conducted within the Senate Judiciary Committee over the past five months. This story could appropriately be named: **THE CASE OF THE SNOOPING STAFFERS AND PEEKING POLITICOS**. The facts of this case are quite simple. In November 2003, conservative papers and a website— the *Wall Street Journal* editorial page, the *Washington Times* and the Coalition for a Fair Judiciary – published excerpts from 19 internal staff memoranda to Democratic Members on the Senate Judiciary Committee. As with so many computer security breaches, these leaked memoranda were just the tip of the iceberg.

---

<sup>1</sup> The author is the 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 also served as the General Counsel on the U.S. Senate Judiciary Committee for Senator Patrick J. Leahy (D-VT). A version of this paper was presented orally at the Yale Law School Conference on Cybercrime and Digital Law Enforcement, “Digital Cops in Virtual Environment,” on March 27, 2004.

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.<sup>2</sup> The report of the inquiry revealed that a staffer for Senator Hatch and a staffer for Majority Leader Frist had for almost 18 months on a daily basis methodically accessed files of targeted Democratic staffers working on judicial nominations and taken almost 4700 documents.<sup>3</sup> 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 by keeping the stolen documents in a zipped (i.e., compressed), password-protected folder on the Hatch staffer’s computer.<sup>4</sup> The Committee file server was shared by both Democrats and Republicans, with each staffer having his or her own account. 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.<sup>5</sup> At least that is how the permissions had worked, were understood to work, and were supposed to work. When a new systems administrator was hired in 2001, he did not set the permissions correctly for over half of the staff on the Committee, so the files in those accounts were accessible to any user with access to the server.<sup>6</sup>

One might think the discovery that Republican staffers were spying on 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 this spying was an appalling breach of confidentiality and custom on the Committee.

There has been public debate, however, about whether a crime has been committed, which is somewhat ironic since this incident happened on the Committee responsible for crafting the original Computer Fraud and Abuse Act (“CFAA”) and every amendment to that law for the past decade.<sup>7</sup> Was the unauthorized access by the Republican staffers simply immoral or was it a crime?

Former White House Counsel C. Boyden Gray, former Majority Leader Trent Lott, and others, have asserted that there was no “hacking” since the security settings on the Committee file server were negligently set, providing easy access. Yet, a plain reading of the prohibitions in the CFAA make clear that unauthorized access and exceeding authorized access of “protected computers”<sup>8</sup> are barred. “Hacking” is not a defined term nor even used in that law, which also contains no requirement that data be

---

<sup>2</sup> Report to the U.S. Senate Committee on the Judiciary by Sergeant of Arms Bill Pickle, March 4, 2004, at p. 7 (hereafter “Pickle Report”). The inquiry was necessarily limited since the Sergeant of Arms has no subpoena powers.

<sup>3</sup> Pickle Report, at p. 9.

<sup>4</sup> *Id.*, at p. 8.

<sup>5</sup> *Id.*, at p. 18.

<sup>6</sup> *Id.*, at p. 11.

<sup>7</sup> 18 U.S.C. § 1030.

<sup>8</sup> See 18 U.S.C. § 1030 (e) (2).

secured and inaccessible.<sup>9</sup> This statute imposes misdemeanor criminal liability for merely obtaining computer information without authorization or by exceeding authorized access.<sup>10</sup> In other words, a Committee staffer may be authorized to access certain files archived on the server for certain purposes by the Member for whom that staffer is employed, but this authorized access is limited and does not cover the dissemination of private, confidential information from the archived files of other Senators' offices. The latter activity would exceed any such limited authorized access and would likely constitute a violation of the statute.

In addition to potentially facing a misdemeanor violation, the Republican staffers may have civil liability problems as well. The CFAA authorizes civil actions for compensatory damages or injunctive relief by any person who suffers any "damage," which is defined to mean any impairment to the integrity or availability of data,<sup>11</sup> or 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.<sup>12</sup> In other words, the staffers who obtained unauthorized access to the Democratic staff memoranda may be subject to civil suit for damages, including by the Senate, which has incurred expenses in the investigation into what happened, including the costs of personnel time in the office of the Sergeant of Arms and for a forensic examination of the systems involved.

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.

The scope of what is covered by the undefined term "access without authorization" and "exceeds authorized access" may be quite broad, leaving enormous discretion to prosecutors. In a politically charged matter, such broad discretion may be both an unwelcome and uncomfortable circumstance. One commentator recently noted, "If 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."<sup>13</sup>

---

<sup>9</sup> 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, in 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, in 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 accessor is not entitled to obtain or alter.

<sup>10</sup> 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.

<sup>11</sup> 18 U.S.C. § 1030 (e) (8).

<sup>12</sup> 18 U.S.C. § 1030(g) and 1030(e) (11).

<sup>13</sup> Assistant Professor Joseph Metcalfe, University of Oregon School of Law, Cybercrime Posting, March 22, 2004, [hermes.circ.gwu.edu/archives/cybercrime.html](http://hermes.circ.gwu.edu/archives/cybercrime.html).

The Pickle Report stopped short of making any recommendations for referral of individuals for criminal violations, but did outline the relevant elements of potentially applicable criminal offenses.<sup>14</sup> The matter has now been referred to the Justice Department by a bipartisan group of Members. The ending to this story must await the prosecutors' decision as to whether a crime was committed.

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 is called the **CASE OF THE PARENTAL NIGHTMARE**.

It starts one morning just a few months ago, when a suburban Mom had her morning coffee 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,<sup>15</sup> 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 uploaded 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 – 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.

P2P file sharing programs make distribution a passive act, but no less subject to criminal liability. People 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.<sup>16</sup>

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 actively posting child porn images to any sites? Or, instead, was he merely a passive distributor by virtue of having downloaded the illegal images into a KaZaa shared folder, with the program doing the active work? The answers to these questions could be helpful in the defense of their son to persuade a

---

<sup>14</sup> Pickle Report, at p. 13, 59-62.

<sup>15</sup> Source: Kazaa website, <http://www.kazaa.com>

<sup>16</sup> 18 U.S.C. §1470.

prosecutor not to charge him, but finding those answers required the services of a computer forensic examiner.

The child porn possession crime is so strict, however, forensic examiners and even attorneys have to be careful not to have these images in their possession. The law treats child porn essentially like heroin – the mere possession, even on behalf of a client to assist in an investigation or defense – is no exception to the crime.<sup>17</sup> 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. Our 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.

While we still do not know the end of the story of the **Peeking Politicos**, the story of the **Parental Nightmare** was a happy one, since the prosecutor declined to prosecute the juvenile.

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 another client machine, and then making the decryption key available at “Free sites,” along with pointers to where the material may be found.<sup>18</sup> 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.<sup>19</sup>

P2P networks actually make the work of investigators fairly easy, since they can track who is sharing illegal files and how much distribution is occurring.<sup>20</sup> In the digital world, users of peer-to-peer 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.<sup>21</sup>

Not every computer crime case is as easy to investigate as many of those on peer-to-peer networks, as demonstrated by the next story of **THE CASE OF THE WIFI**

---

<sup>17</sup> 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.

<sup>18</sup> Geoff Fellows, “Peer-to-Peer Networking Issues-- An Overview,” *Digital Investigation, The International Journal of Digital Forensics & Incident Response*, vol. 1, at pp. 3-6 (February, 2004).

<sup>19</sup> *Id.*, at p. 6.

<sup>20</sup> *Id.*, at p. 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.”)

<sup>21</sup> While criminal copyright liability requires a “willful” intent, civil infringement liability is strict.

**SPOOFER.** For over two years a company was the target of embarrassing e-mails containing derogatory and sexually explicit 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. Clients, who received these disturbing spoofed e-mails, got upset, particularly when the company appeared to be incapable of stopping them. The company lost thousands of dollars as clients took their business elsewhere.

The e-mail header information on the e-mails showed the originating IP addresses which the FBI attempted to trace. However, the traces led not 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 from 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 the default setting of no security features enabled, and many users do not bother, or do not know how, to change the default settings on the equipment. Accordingly, 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 anonymizing method for the perpetrator.

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 account to access a proxy server to conceal the originating IP address of the computer he was using within the University computer lab, and use that proxy server to access e-mail accounts from which he sent spoofed e-mails.

Almost two years into this expensive harassment, the company turned to us 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, 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.

We also found that senior executives at a sister company of the targeted company had been sent 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. He 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 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. 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 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 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 – as certain originating emails.

The FBI then arrested him. When the defendant’s house in Maryland was searched they found numerous firearms, explosives and chemicals, as well as a recipe for the production of a deadly toxin. He has been detained pending trial. As noted before, 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 targeted company. After two years of being victimized, it took the concerted

investigative effort of the FBI, 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 Computer Fraud and Abuse statute 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, including, for example, over "spyware." Care must be taken to ensure that legitimate and other self-help activities are not impaired by regulatory measures written so broadly they suffer from the same scope questions raised by the CFAA.

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.