ARTICLE

"A CASE OF IDENTITY"[1]: A GAPING HOLE IN THE CHAIN OF EVIDENCE OF CYBER-CRIME

BY JOEL MICHAEL SCHWARZ[2]

---

[1] SIR ARTHUR CONAN DOYLE, *Adventures of Sherlock Holmes, in* THE COMPLETE SHERLOCK HOLMES, 159, 190 (Doubleday & Co. 1930).

[2] Trial Attorney, Computer Crime and Intellectual Property Section ("CCIPS"), U.S. Department of Justice. Previously, Special Counsel for Internet Matters, Investor Protection & Securities Bureau, and Assistant Attorney General, Internet Bureau, New York State Attorney General's Office. This article was authored by Mr. Schwarz, in his individual capacity, prior to his joining CCIPS. The views expressed in this article are those of the author and do not necessarily represent the views of the United States. The author would like to gratefully acknowledge the contributions of Martha Stansell-Gamm and Christopher Painter.

I. INTRODUCTION

As the most famous fictional detective of all time, Sherlock Holmes, once observed, "there is no branch of detective science which is so important and so much neglected as the art of tracing footsteps."[3] Despite the passage of over a hundred years, from late nineteenth century England to early twenty-first century America, Sherlock Holmes' words still ring true. Tracing footprints remains as important a crime-solving art today at it was in Holmes' time. The difference is that while Holmes' task was to trace footprints through the streets and back-alleys of London, detectives now trace the virtual footprints left on the roads and backbones of the Information Superhighway.

"Footprints on the Internet?" you may ask. Elementary my dear Watson! While a recent spate of alleged privacy violations by various companies has helped to alert the public that Internet sessions are not as anonymous as initially believed, most people fail to appreciate exactly how personal information on the Internet is captured and used.[4] Generally speaking, a person creates a record of activity from the moment that person logs on to the Internet, from every Web site that the person visits to every e-mail that the person sends. This record of activity—these "virtual footprints"—captured by one or more computer servers, forms a vital part of the forensic science that enables law enforcement to trace and apprehend individuals engaged in Internet crime. The problem today, however, lies not with tracing these footprints, but rather with determining the identity of the individual on the other end of those footprints.

As a general rule, sophisticated Internet criminals are aware of the anonymity provided by the Internet, and the difficulties law enforcement faces in piercing this veil. As a result, these criminals adjust their activities to

---

[3] SIR ARTHUR CONAN DOYLE, *A Study in Scarlet*, *in* THE COMPLETE SHERLOCK HOLMES, 15, 84 (Doubleday & Co. 1930).

[4] *See, e.g.*, Press Release, Federal Trade Commission, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), *at* http://www.ftc.gov/opa/2002/08/microsoft.htm (regarding FTC charges that Microsoft misrepresented the security and privacy of Microsoft's "Passport" Internet service); Press Release, Federal Trade Commission, Popcorn Company Settles FTC Privacy Violation Charges (Feb. 14, 2002), *at* http://www.ftc.gov/opa/2002/02/popcorn.htm (regarding FTC charges that American Pop Corn Company collected information from children without parental consent, which is a violation of the Children's Online Privacy Protection Rule); Press Release, Federal Trade Commission, Eli Lilly Settles FTC Charges Concerning Security Breach, (Jan. 18, 2002), *at* http://www.ftc.gov/opa/2002/01/elililly.htm (regarding FTC charges that Eli Lilly disclosed consumers' e-mail addresses); Press Release, Federal Trade Commission, FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm (regarding FTC charges that Toysmart sold consumer information to third parties in violation of an agreement forbidding this sale).

maximize this anonymity while online. For example, a criminal might provide fictitious account registration information to open a free ISP account[5] and then use stolen credit card numbers to make online purchases. Under these circumstances, the information provided by the criminal himself will usually be of little use in uncovering his true identity. The only valuable evidence will be the "virtual footprints" left behind by the criminal. Investigators can use these footprints to trace back to the telecommunications connection and computer terminal from which the acts originated, and thus, hopefully, pierce the criminal's anonymity. Knowing this, a sophisticated Internet criminal will further mask his identity by using publicly available computer terminals such as those found at a public library, Kinko's or Starbucks.[6] In such a case, the trail of virtual footprints will potentially lead to a dead-end because law enforcement will not be able to ascertain the identity of the individual who created those footprints.

In essence, a case may turn on an investigator's ability to trace a criminal's virtual footprints back to the terminal used and, hopefully, the criminal's doorstep.[7] Conversely, without these virtual footprints, and the ability to attribute them to real-world contacts, Internet crime fighting becomes a much more difficult—if not impossible—proposition.

This article begins by discussing the technology implicated during a typical Internet session. To illustrate the utility of virtual footprints in solving Internet crimes, the article then reviews the investigation and prosecution of a securities fraud perpetrated over the Internet in which the perpetrator's virtual footprints served as the primary evidence in uncovering his identity.[8] Investigators caught the perpetrator by tracing the footprints back to his home and work addresses.[9] The article then examines the identification problems that arise when a criminal uses publicly available computer terminals, and offers two options for resolving this problem: the introduction of legislation and industry self-regulation. Both options would require the collection and maintenance of user identification information as a pre-condition for terminal usage. In considering the possibility of using legislation to proscribe the criminal use of publicly available computer terminals, the article reviews and analyzes other legislative and rule-making attempts at using identification mechanisms as a means of deterring and fighting criminal activity. As a corollary to this

---

[5] For simplicity, any reference in this article to an ISP shall mean Internet service providers, web host providers and e-mail providers that provide either pay or free services.

[6] Kinko's and Starbucks are only two examples of some of the commercial establishments that offer computer terminals to the public for a fee. This list is by no means meant to be an exhaustive list of such establishments.

[7] *See, e.g.*, Christopher M.E. Painter, *Tracing in Internet Fraud Cases: PairGain and NEI Webworld, at* http://www.cybercrime.gov/usamay2001_3.htm (last modified July 9, 2001).

[8] *See id.*

[9] *See id.*

analysis, the article distinguishes commercial public terminals—i.e., those for which a person must pay to use--from free public terminals—such as those available at the public library. The article next examines the privacy implications of mandating providers of commercial public terminals to request and maintain photo identification of consumers before allowing use of the computers. Finally, the article concludes that the implementation of a mechanism that enables law enforcement to identify public terminal users is necessary to deter and prosecute criminals who would use the anonymity of the Internet to engage in cyber-crime.

II. A TECHNOLOGY PRIMER

A. IP Addresses

Every computer on the Internet has an Internet Protocol ("IP") address.[10] An example of an IP address is 207.25.71.28; four numbers separated by three periods.[11] Akin to a person's Social Security number, an IP address uniquely identifies every computer on the Internet.[12]

An IP address can be either static or dynamic.[13] A static IP address identifies a particular computer over its operating lifetime.[14] In certain cases, computers connected to the Internet with a cable modem or a DSL modem have static IP addresses.[15] Static IP addresses are also frequently assigned to corporate or university computer systems that operate with a continuous Internet connection. In the case of corporate or university computer networks, many of these organizations mask the IP addresses of their internal computers from computers outside the Intranet by using a proxy server.[16] While computers within the network can identify the IP addresses of their peers, the proxy server often functions as a security gate and firewall between the internal network and the public Internet.[17] To accomplish this, a proxy server substitutes its own IP address for the IP addresses of its subordinate computers

---

[10] See Shawn C. Helms, Translating Privacy Values With Technology, 7 B.U. J. SCI. & TECH. L. 288, 295 (2001).

[11] *See* Joel Michael Schwarz, International Use of U.S. Corporate Intranets: Legal Risks and How to Avoid Them, 20 ACCA Docket No. 2, 28, 32 (2002). *See also*, British Telecomms. PLC v. Prodigy Communications Corp., 217 F. Supp. 2d 399, 407 (S.D.N.Y. 2002) (offering a description of IP addresses).

[12] *See British Telecomms.*, 217 F. Supp. 2d at 407.

[13] *See* Helms, *supra* note 10, at 295.

[14] *See id.*

[15] *See id.* at 295 n.41.

[16] *See* Schwarz, *supra* note 11, at 31-32 (2002). *See also* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1061 (N.D. Cal. 2000) (describing proxy servers).

[17] *See* Helms, *supra* note 10, at 316.

behind the firewall, thus preserving their anonymity by masking their IP addresses from anyone outside on the Internet.[18] Interestingly, at the time traffic passes into and out of the proxy server/firewall, the proxy server often captures the source and destination IP addresses, thereby giving rise to a virtual footprint.

A dynamic IP address, on the other hand, is an IP address usually assigned to a computer by an Internet Service Provider ("ISP") such as America Online or EarthLink.[19] The ISP assigns a dynamic IP address to a user's computer when the user logs into the ISP through a dial-up modem.[20] Dynamic IP addresses are generally unique to a given user only for the length of that user's session.[21] When the user signs off, the ISP assigns the IP address to a different user. More importantly, the ISP stores the start and end times of the user's session, along with the user's username and the IP address assigned to that user for that particular session, again creating a virtual footprint.[22]

B. RADIUS Logs/Automatic Number Identification ("ANI") Logs

In order for a user to log into a chosen ISP using a dial-up modem, the user must first select a phone number provided by the ISP, usually a local access number. This local access number connects to ISP servers responsible for receiving calls, assigns the user's computer a dynamic IP address, and then provides the user with Internet access. These servers are known as the ISP's Points of Presence, or POPs.[23]

Whenever a user dials into a POP, the POP usually has the ability to identify the phone number from which the user is calling, akin to caller-ID.[24] If the ISP chooses, the ISP can usually capture these phone numbers in Remote Authentication Dial-in User Service ("RADIUS") logs, also referred to as Automatic Number Identification ("ANI") logs.[25] This is yet another example of a virtual footprint.

C. Web Server Logs

As previously discussed, every computer on the Internet has an IP address.[26]

---

[18] *See* Schwarz, *supra* note 11, at 32.

[19] *See* Helms, *supra* note 10, at 295.

[20] *See* Painter, *supra* note 7.

[21] Some ISPs actually use dynamic IP addressing within a user session, meaning that the user's IP address is dynamically changed by the ISP during a single session, and thus a user might have multiple IP addresses during that session.

[22] *See* Helms, *supra* note 10, at 295 n.43.

[23] *See* GTE.net LLC v. Cox Communications, Inc., 185 F. Supp. 2d. 1141, 1142 (S.D. Cal. 2002) (describing Points of Presence).

[24] *See* Painter, *supra* note 7.

[25] *See id.*

[26] *See* discussion *supra* Part II.A.

Some computers have static IP addresses that remain with them at all times, while others have dynamic IP addresses assigned for the length of an Internet session. Some have their true IP addresses masked by a proxy server. Regardless of how a computer gets an IP address, however, those addresses are absolutely vital for purposes of conducting an Internet session. Without an IP address, a computer cannot maintain a conversation with any other computer over the Internet, because all information sent between the two computers must contain the source and destination IP addresses (i.e., the IP addresses of the sending and receiving computers) in order to be properly routed between the two. Just as the United States Postal Service cannot deliver a letter without a street address, computers cannot deliver information over the Internet without an IP address.

So what does this have to do with Web servers? Elementary, my dear Watson. Web servers are computers set up to host Web pages (i.e., to permit people to access a Web site for informational and/or transactional purposes). A Web server, much like one's personal computer, has an IP address. Thus, when a user accesses a Web site, the user's request is sent to the computer hosting that Web site (the Web server) using its IP address. This "asks" the server to open a session on the user's computer, which provides the IP address with the request.[27] The Web server then captures your IP address and returns the requested Web page to that address.[28] When you request another Web page, you send another request to the Web server, using the Web server's IP address, and the Web server again returns a Web page to you, using your computer's IP address.[29] This dialogue continues for the length of your session on that Web site.[30] When you exit the Web site, or close the browser window, the session ends.[31]

Because a Web server often maintains sessions with several computers at once, the Web server must identify the computer to which it is sending the requested information. The Web server will usually capture the IP addresses of every computer with which it is carrying on a session, thereby enabling it to differentiate one session from another. These IP addresses are in turn maintained in Web server logs--computer files designed to record and store the IP addresses of every computer that accesses the Web site. If you access amazon.com, for example, one of Amazon's Web servers will likely capture your IP address. If you log-in to your Hotmail account by going to hotmail.com, chances are that a Hotmail Web server will capture your IP address. Any time that you access a Web site, chances are that one of the site's

---

[27] *See* Marshall Brain, *How Web Servers Work*, HOW STUFF WORKS, *available at* http://www.howstuffworks.com/web-server.htm (last visited Jan. 29, 2003).

[28] *See id.*

[29] *See id.*

[30] *See id.*

[31] *See id.*

web servers is going to capture your IP address and write that information to some type of log file; creating additional virtual footprints.

III. PAIRGAIN CASE

Having reviewed some of the ways that virtual footprints are created, we can now look at how those footprints are used in Internet crime fighting. *United States v. Hoke*, the first major case of Internet stock manipulation in the United States, best illustrates the vital role of virtual footprints.[32] This 1999 case demonstrated how the footprints created during a securities fraud scam perpetrated over the Internet figured into the investigation of the crime and the apprehension of the perpetrator.

In *Hoke*, a message was posted by an individual using the name Stacey Lawson, of Knoxville, Tennessee, on bulletin boards hosted by Yahoo! Finance and other companies.[33] According to the message, an Israeli company was planning to purchase PairGain, a telecommunications equipment company traded on the NASDAQ, for 1.35 billion dollars.[34] This message also contained a link to a purported Bloomberg news story.[35] Although the Web page to which the message linked appeared to be an authentic Bloomberg Web page, the page was in fact fictitious, as was the story of the impending purchase of PairGain by the Israeli company.[36] The false story triggered a buying spree and the PairGain stock rose an impressive 31% in just two hours, approximately ten times its normal volume.[37] Inevitably, the hoax was exposed. This sent the stock plummeting, causing substantial loses by thousands of unsuspecting victims.[38]

The federal and state law enforcement authorities immediately began their investigations of this crime after the hoax became apparent.[39] The cyber investigation began by focusing on the message posted to the Yahoo! bulletin board, as well as on the fake Bloomberg Web page.[40] Unfortunately, neither source was in itself very revealing. The information provided by Hoke to open

---

[32] CR 99-441 (C.D. Cal. Indictment filed Apr. 30, 1999). *See also* Painter, *supra* note 7, at 2.

[33] *See* Painter, *supra* note 7, at 2.

[34] *See id.*

[35] *See id.*

[36] *See id.*

[37] *See id.*

[38] *See id.*

[39] *See id.*

[40] *See id.*

the Yahoo account was false, as is not uncommon when individuals open these free ISP accounts.[41] Investigation also revealed that the fake Bloomberg Web page had been posted by someone using an account opened with a free Internet Web hosting service called Angelfire.[42] However, since Angelfire is also a free service, and users are able to open accounts by providing only rudimentary information, the information provided to Angelfire was likewise false.[43] In registering with Angelfire, users are asked to provide an e-mail account contact, after which a password is e-mailed to the new user. The e-mail account provided to Angelfire in this case was a Hotmail account, which again contained bogus account registration information.[44]

To the layman, it would seem that Hoke had utilized the anonymity of the Internet, and the wide availability of free Web hosting and e-mail accounts, to perpetrate the perfect crime. But alas Watson, we return to Holmes' theory: "there is no branch of detective science which is so important and so much neglected as the art of tracing footsteps."[45] The perpetrator of this crime had indeed left a number of virtual "footprints." They simply needed to be discovered, and then traced back to the doorstep or, in this case, the computer of the perpetrator.

Although the perpetrator had provided false, unverified registration information to Yahoo!, Angelfire and Hotmail, the perpetrator still had to log in to those sites in order to register and provide that false information.[46] In doing so, the perpetrator stood at the virtual front door of each of those Web sites, leaving his virtual footprints for the cyber-savvy investigator to find.

Angelfire, like most Web sites, captured Hoke's IP address when he logged in to register for an account and to create the fake Bloomberg Web page, as well as every time he modified that Web page.[47] As discussed previously, these logs are known as Web server logs.[48] In this particular case, Angelfire's Web server logs (i.e., Hoke's "footprints") showed that Hoke had accessed his account from several different IP addresses in the month and a half preceding the crime. By looking up these IP addresses on various listing services available on the Internet, "it was determined that the numbers corresponded to computers at PairGain (static IP numbers) and at Mindspring, a large ISP (dynamic numbers)."[49] In other words, investigators followed Hoke's virtual footprints. Hotmail also maintained Web server logs, which indicated that

---

[41] *See id.*

[42] *See id.* at 2-3.

[43] *See id.*

[44] *See id.*

[45] *See* DOYLE, *supra* note 3, at 84.

[46] *See* Painter, *supra* note 7, at 3.

[47] *See id.*

[48] *See* discussion *supra* Part II.C.

[49] *See* Painter, *supra* note 7, at 3.

Hoke had accessed his Hotmail account from IP addresses that were registered to PairGain and Mindspring.[50] The investigators issued a subpoena to Mindspring requesting the identity of the user account that used those Mindspring IP addresses to access Angelfire and Hotmail on the relevant date and times.[51] In every instance, Mindspring identified that account as having the username "ghoke."[52] Of course, there was the possibility that someone had hacked into the "ghoke" account and used that username inappropriately. However, this is where the next footprint came into play.

Mindspring also maintained logging information called "radius logs," which indicated that the phone number used to dial into Mindspring's service when accessing the "ghoke" account was registered to a phone belonging to Gary Hoke.[53] Finally, Hoke had also logged into his Angelfire and Hotmail accounts from an IP address registered to PairGain.[54] As it turned out, Hoke was an employee of PairGain, working out of the Raleigh, North Carolina branch office.[55] PairGain, like most companies, would have likely used a proxy server/firewall that creates log files of information passing into and out of the company's Intranet.[56] Since Hoke also logged into Angelfire and Hotmail from his computer inside of PairGain, PairGain would have presumably captured this traffic in their firewall logs, and would have traced those logs back to the computer terminal in Hoke's office.[57]

With the help of all of these virtual footprints Gary Hoke was identified and arrested.[58] Hoke eventually pled guilty to securities fraud, thereby ending one of the first high-profile Internet securities fraud cases in the country; a case, which at first blush, appeared to be impossible to solve because of the anonymity of the Internet and the use of free ISP accounts. More importantly, it involved a defendant who would likely have never been identified without the benefit of these virtual footprints.

IV. THE ELECTRIC COMMUNICATIONS PRIVACY ACT

The Electronic Communications Privacy Act (the "ECPA"), passed in 1986, was one of Congress' earliest attempts to balance the evolving needs of law enforcement to access electronically stored evidence with the public's desire

---

[50] *See id.*
[51] *See id.*
[52] *See id.*
[53] *See id.*
[54] *See id.*
[55] *See id.*
[56] *See id.*
[57] *See id.*
[58] *See id.*

for privacy.[59] The purpose of ECPA was to facilitate law enforcement's access to certain electronic records, using various means of legal processes, depending upon the type of information being accessed and the level of privacy protection that a user might expect applied to such information.[60] As the Department of Justice explains in its manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, "[t]he structure of ECPA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw different privacy interests at stake in stored e-mails than in subscriber account information."[61]

Pursuant to ECPA, a law enforcement agency must use different legal processes to secure records pertaining to an individual's Web surfing habits, known as "transactional records," as opposed to the content of that individual's communications.[62] The specific process used depends upon the privacy interest in the information sought. For example, if a law enforcement agency wishes to secure "basic subscriber information," the least invasive type of information from a privacy perspective, the law enforcement agency need only serve a statutorily authorized law enforcement subpoena on the ISP in possession of these records.[63] "Basic subscriber information" includes:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account

---

[59] United States Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual*, *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (July 2002) (explaining that while the Fourth Amendment guarantees individuals a constitutionally protected right against unreasonable government intrusions into their privacy, the Fourth Amendment generally does not protect the privacy of information disclosed to third parties. The Fourth Amendment was not deemed to apply to information sent by an individual through her ISP because in sending that information she necessarily discloses that information to her ISP (i.e., a third party). Nonetheless, Congress realized that if communications sent via public ISPs were not protected against voluntary disclosure to law enforcement, the growth of this burgeoning industry could be jeopardized. As such, Congress enacted ECPA to create a statutory right of privacy in this information, to pick up where the Fourth Amendment left off.)

[60] *See id.*

[61] *See id.*

[62] *Compare* 18 U.S.C. § 2703(a) (2000) *with* 18 U.S.C. § 2703(d) (2000).

[63] 18 U.S.C. § 2703(c).

number).[64]

Under ECPA, a law enforcement subpoena is the easiest method for gaining access to ECPA-protected records and requires the least amount of judicial intervention.[65] On the other hand, if a law enforcement agency wishes to secure the content of a subscriber's e-mail communications, a court-ordered search warrant is necessary. In other words, the more personal the information, the greater the legal burden on law enforcement to secure that information.[66]

In addition to being able to secure various types of electronic records from ISPs, ECPA also provides law enforcement with a mechanism with which to preserve these records pending issuance of proper legal process. Specifically, "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."[67]

ECPA offers an example of Congress' efforts to adjust to technological changes in facilitating the investigation and prosecution of crime.[68] ECPA is also a prime example of Congress' cognizance of the importance of virtual footprints to successful law enforcement investigations, and the need to be able to track cyber-activity back to real-world individuals.[69] By providing law enforcement entities with these powers, Congress has made a clear policy choice that law enforcement's need for these records in an expeditious fashion outweighs any potential privacy rights or expectations that may exist in this information.

The tools provided by Congress, however, presuppose that the criminal's true identity will eventually be revealed after following all of these virtual "footprints" to the end of the line. In practice, this is not always the case. For example, when an Internet criminal commits crimes from a publicly available computer terminal, it is extremely difficult, if not impossible, to attribute this conduct to a specific individual on a specific date and time because that terminal is potentially accessed by the entire population. In order to ensure the

---

[64] *Id.* at 2703(c)(2).

[65] *See* 18 U.S.C. § 2703(c).

[66] *See* 18 U.S.C. § 2703(a).

[67] 18 U.S.C. § 2703(f).

[68] *See* S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 (describing how legislative efforts to combat crime must recognize changes in technology, citing the telephone as an example).

[69] Statement of Senator Patrick Leahy, Ranking Member, Senate Committee on the Judiciary, *Joint Senate-House Hearing On "Internet Denial of Service Attacks and the Federal Response" available at* http://leahy.senate.gov/press/200002/000229b.html (Feb. 29, 2000) (describing computer-related crime as one of law enforcement's greatest challenges, and that computer crime laws must be updated in order to meet this challenge).

apprehension and prosecution of sophisticated Internet criminals and terrorists who use these terminals to commit their crimes, there must be a way to trace this type of computer use back to an individual actor.

V. PUBLICLY AVAILABLE INTERNET COMPUTER TERMINALS - THE PROBLEM FROM A LAW ENFORCEMENT PERSPECTIVE

Borrowing a phrase coined by the telecommunications industry, the problem with the use of publicly available Internet computer terminals (hereinafter "public terminals") by criminals, such as those available at cyber-cafés and printing facilities such as Kinko's, comes down to the issue of "the last mile."[70] As discussed previously, the goal of any Internet crime investigation is to identify the actual perpetrator of a crime, or at least the computer terminal used by the perpetrator.[71] Since a private computer terminal is generally accessible to only a few people, identifying the terminal usually leads to the identification of the target or a select group of targets.[72]

In the *Hoke* case, for example, once alerted to the fact that they had a criminal in their midst, PairGain likely identified Hoke's work computer through their firewall logs.[73] In the case of a private computer terminal available to a select group of people (e.g., a terminal in a home, or even at a high school), identification of the actual terminal used permits the investigator to engage in real world investigative techniques at the scene of the crime. These techniques include searching for fingerprints, speaking to witnesses near the scene at the time of the crime, examining a list of people who potentially had access to the computer terminal, assessing who had the means and motive to commit the crime, and then interviewing those potential targets.[74] In other words, when a crime is committed from a private terminal with limited access, there is usually a way to trace the criminal activity over that "last mile" back to

---

[70] *See* James P. Speta, *Handicapping the Race for the Last Mile?: A Critique of Open Access Rules for Broadband Platforms*, 17 YALE J. ON REG. 39, 46 (Winter 2000) (describing the "last mile" as the physical barrier between the user and the nearest aggregation point). Here the "last mile" is the connection between the computer terminal and the criminal who used that terminal.

[71] *See, e.g.*, Jason Vaughan & Brett Burns, *Bringing Them in and Checking Them Out: Laptop Use in the Modern Academic Library*, 21 INFORMATION TECHNOLOGIES & LIBRARIES 3, *available at* http://www.lita.org/ital/2102_vaughan.html (June 2003) (noting that, in general, a library's staff tries to trace Internet crime on its computers to the perpetrator instead of trying to anticipate and block all forms of malicious behavior that involves the use of the library's resources).

[72] *See id.*

[73] *See* Hoke, *supra* note 32.

[74] *See generally* National Institute of Justice, *Crime Scene Investigation: A Guide for Law Enforcement*, *available at* http://www.ojp.usdoj.gov/nij/pubs-sum/178280.htm (Jan. 2000).

the criminal.[75]

When a criminal uses a public terminal to commit a crime over the Internet, however, this "last mile" becomes more illusory. Generally, there is no identification required, nor any record-keeping conducted, when a person uses a public terminal. Thus, the "last mile" will often prove to be an insurmountable obstacle for cyber investigators. Moreover, many of the investigative techniques that an investigator can use with a private terminal will be of much less utility when utilized with a public terminal. For example, dusting for fingerprints is more difficult because access to the public terminal is broader, meaning that the fingerprints may yield an overabundance of potential suspects.[76] Similarly, as no identification was secured and no records were created, investigators often cannot build a list of who might have had access to the public terminal on a given date and time.[77] While it is not impossible to perform such investigation, it is much less likely to be fruitful. Internet criminals know this and often rely upon this added level of anonymity to commit Internet crime using public terminals.[78]

In the *Hoke* case, for example, if Hoke had only logged into his Angelfire and Hotmail accounts using public terminals, the two primary pieces of evidence that directly linked Hoke to the crime, namely IP addresses that traced back to his home and office, would not have existed.[79] If Hoke had logged in from a public terminal at a Kinko's (which does not generally require any identification or record keeping), investigators would have traced that "last mile" back to the Kinko's computer terminal--a terminal that the entire population had access to at any given time. In other words, in all likelihood Hoke would not have been captured or convicted.

Thus, maintaining records of the users of public terminals serves a vital law enforcement purpose. Of course, there may be other ways to track criminals who use the Internet to commit crime. For example, the old law enforcement adage of "follow the money trail" still applies to crimes committed over the Internet, as does the use of other types of physical evidence such as fingerprints at the scene, witness identification, and so forth. Nonetheless, in some cases there may be little if no physical evidence to follow, in which case the virtual footprints of the criminal may be the only clue available to law

---

[75] *Cf.* Vaughan & Burns, *supra* note 71, at 3 (discussing one way to associate a patron with a given cyber-attack).

[76] *Cf. Crime Scene Investigation*, *supra* note 74 (describing how a typical crime scene investigation proceeds).

[77] *See id.* (noting the importance of building a list of individuals present at a crime scene).

[78] *See, e.g.*, Phil Hirschkorn, *FBI Explains Missing Moussaoui E-mail*, *available at* http://www.cnn.com/2002/LAW/09/04/moussaoui.computer/index.html (Sept. 4, 2002), (illustrating how suspected 9/11 conspirator allegedly used computer at Kinko's to send and receive e-mail).

[79] *See* Hoke, *supra* note 32.

enforcement officials.

As such, in order to track the use of a public terminal, an identification and record-keeping system needs to be developed. This program—a program that will verify user identification and maintain a file copy of the identification presented—can be referred to as a "credentialing program."

In proposing a credentialing program, an important distinction should be drawn: tracking or monitoring the specific activities of a public terminal user while Web surfing is not the goal of the credentialing program; nor is the goal to require proprietors of public terminal establishments to engage in additional oversight of an individual once the individual is properly credentialed.[80] Rather, the narrower goal of the program is to verify the identity of an individual using a public terminal and to maintain a record of this identification for some minimal period of time. If a crime is then committed using that terminal, law enforcement can follow the leads back to that terminal and, then, to the individual perpetrator.[81]

Moreover, in suggesting potential solutions to this problem, this article takes no position on whether such a strategy should be implemented via voluntary self-regulation, or through the introduction of legislation. The purpose of this article is solely to illustrate the problem in an attempt to initiate a dialogue between industry and law enforcement on how to address the situation.

VI. WHO TO INCLUDE IN THE SOLUTION AND WHO TO EXEMPT

Before crafting a credentialing mechanism, the first step is deciding whether all public terminals should be treated in the same manner. Generally speaking, there are two types of public terminals that individuals may use to access the Internet: commercial pay-for-use public terminals (hereinafter "commercial public terminals"), such as those found at a Kinko's or a cyber-café, and free public terminals, such as those found in libraries.[82] When deciding whether to include a category of public terminals in a credentialing program, it is important to consider the administrative and monetary impact that such a proposal might have on each, bearing in mind that the impact may differ

---

[80] *See generally* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085 (2002) (offering an examination of how the state must maintain constitutional privacy protection for electronic information).

[81] *Cf.* Vaughan & Burns, *supra* note 71.

[82] *See, e.g.*, KINKOS.COM, *Computers & Facilities: Computer Rentals*, http://www.kinkos.com/our_services/store_services/computer_rentals/php (indicating that computers are available to rent); CYBERCAFES.COM, *About Cybercafes*, http://www.cybercafes.com (listing available cyber cafes by geography); Miles Fidelman, *All-Out Internet Access: The Cambridge Public Library Model* (Feb. 1997), http://civic.net/library.html (describing the use of Internet workstations in a public library setting).

depending on the category of terminal. A brief discussion of the categories may help illustrate this point.[83]

A. Commercial Public Terminals

The additional administrative overhead that would be borne by proprietors of establishments offering purely commercial public terminals, like Kinko's and cyber-cafes, appears to be minimal. These types of establishments already track users in order to charge them for their public terminal usage.[84] The proprietor of an establishment offering these types of commercial public terminals usually requires a user to request the assignment of a terminal.[85] The time that the user begins using the terminal and the specific terminal used are recorded.[86] When finished, the user informs the proprietor, or the cashier designated to handle payment for terminal usage, who in turn collects the amount due.[87] In general, the charges for use of a commercial public terminal are based upon some increment of time, such as X dollars for every 10 or 15 minutes of usage.[88]

While commercial establishments may vary this process, nearly all establishments must have a mechanism to track the terminals used, who used them, and for what period of time, in order to calculate the charges assessed against the user.[89] A mandate that requires these establishments to credential users prior to permitting their use of a commercial public terminal, and to maintain a copy of this identification information for some period of time after usage, would not encompass a great deal of additional administrative overhead or monetary cost. In fact, when the person using a commercial public terminal pays with a credit card, debit card, or check, access identification information is simple and direct.[90] Thus, these establishments currently have the means to implement such a program without incurring an additional burden. With

---

[83] *See generally* Patricia F. First & Yolanda Y. Hart, *Access to Cyberspace: The New Issue in Educational Justice*, 31 J.L. & EDUC. 385, 386-90 (2002) (showing the disparity within the United States between those who have access to the Internet and those who do not, and this disparity is referred to as the "digital divide").

[84] *See* KINKOS.COM, *supra* note 82.

[85] *See id.*

[86] *See id.*

[87] *See id.*

[88] *See id.*

[89] *See, e.g.*, CYBERCAFES.COM, *at* http://www.cybercafes.com/city.asp?name=san+francisico (offering an description of charges for Internet access in a cybercafe, using the San Francisco area as an example).

[90] *See* Thomas H. Odom & Gregory S. Feder, *Challenging the Federal Driver's Privacy Protection Act: The Next Step in Developing a Jurisprudence of Process-Oriented Federalism Under the Tenth Amendment*, 53 U. MIAMI L. REV. 71, 109 (1998) (noting that a state drivers license is used as identification in a credit card transaction).

regard to these establishments, perhaps a credentialing program simply requires a tighter and more uniform identification process coupled with the implementation of some type of record keeping system.

In establishing a credentialing program we must also look at the effect that the program might have on the availability of these commercial public terminals to the general public because, as a general policy, greater availability of Internet access should be encouraged. One possible effect of the credentialing program is that, if the cost of implementation is too high, it will no longer be worthwhile for proprietors of these establishments to continue to offer these terminals and the availability of these terminals will decrease. However, the reality of the matter is that proprietors of commercial public terminals maintain these terminals due to the fact that there is an economic incentive to do so. This monetary incentive would be unlikely to wholly disappear after the implementation of a credentialing program.[91] This is especially true in light of the fact that most of the administrative resources needed to implement such a program would already be in place by virtue of the extant business model. While this article will not examine the economic implications of this program in great detail, it should be noted that these establishments also have other options available to them for making up the additional costs incurred as a result of credentialing individuals. For instance, establishments can pass additional costs on to users by raising user fees and/or advertising rates, with price increases being constrained only by the market force of competition from other commercial public terminal establishments.[92]

B. Free Public Terminals

Implementing a credentialing program as a pre-requisite for the use of free public terminals, however, as opposed to commercial public terminals, would potentially involve a substantial administrative and monetary burden on the proprietors of those establishments. As free public terminals are provided without charge, there is generally little need for, or practice of, formal supervision and monitoring. Indeed, the American Library Association's ("ALA") "Freedom to View" statement sets forth a number of fundamental principles within a free society, including the concept that libraries should "provide the broadest access to film, video, and other audiovisual materials because they are means for the communication of ideas."[93]

If we were to require credentialing for the use of free public terminals, the proprietors of these terminals would likely need to hire staff to oversee those

---

[91] *Cf.* John A. Barrett, Jr., *The Global Environment and Free Trade: A Vexing Problem and a Taxing Solution*, 76 IND. L.J. 829, 856 (2001) (showing how importers still have a monetary incentive to import goods into the U.S. even with an environmental import tax).

[92] *See id.* (increased costs from import tax can be passed to the consumer).

[93] American Library Association, *Freedom to View Statement, available at* http://www.ala.org/alaorg/oif/freedomtoview.html (Jan. 10, 1990).

terminals. Credentialing would thereby create an additional monetary expense, and thus a potential disincentive to the offering of public terminals. This would likely result in either a complete loss to the public of the free terminals, or the implementation of a fee-for-use program to cover the additional expenses. After all, why should an establishment provide free Internet access to the public if such access entails significant administrative and monetary burdens?

Interestingly, a national survey conducted in 2000 by the Library Research Center of the University of Illinois at Urbana-Champaign indicated that although there is no formal written library policy mandating monitoring of free public terminals, libraries often place these terminals in areas where librarians can watch.[94] This type of monitoring, however, is different than the type of monitoring that a credentialing program would require. Libraries do not seem to have a formal monitoring policy nor do libraries appear able to conduct the formalized monitoring required by the credentialing program.[95] Nonetheless, if the additional burden to implement the program is kept low, it remains feasible for a public library to implement a credentialing program.[96]

As stated above, the availability of Internet access via public terminals constitutes the second factor that a credentialing program must consider. While implementation of a credentialing program is needed in order to give law enforcement the ability to identify criminals who use public terminals to commit their crimes, we can assume that not every law-abiding citizen will feel comfortable complying with such a program. Indeed, it is inevitable that some law-abiding individuals, individuals who do not engage in criminal activity, will feel uneasy with the potential privacy lost through such a credentialing program.[97]

Moreover, free public terminals are often the only way for low-income families to access the Internet.[98] Free public terminals also present the only viable alternative for those who do not otherwise have access to a computer, or who do not have the requisite photo identification necessary for commercial public terminal usage.[99] By implementing a credentialing program at libraries, we may deter, and in fact prevent, Internet access by the members of the population currently facing significant challenges in accessing the Internet, and

---

[94] Leigh S. Estabrook & Ed Lakner, *Managing Internet Access: Results of a National Survey*, AMERICAN LIBRARY, Sept. 1, 2000, at 60.

[95] *Cf.* Lynn F. Miller, *Big Brother in the Public Library*, NEW JERSEY LAWYER, Feb. 2002, at 29, 31 (discussing the inability of a library to monitor the content of a patron's use).

[96] *Cf.* Cynthia K. Richey, *Molding Effective Internet Policies*, 22 Computers in Libraries 16, (June 2002), *at* http://www.infotoday.com/cilmag/jun02/richey.htm (library reserving the right to require registration before use of the computer).

[97] *See, e.g.*, Miller, *supra* note 95, at 30-31.

[98] *See* First & Hart, *supra* note 83, at 386-90.

[99] *See id.*

thereby potentially exacerbate the "digital divide."[100] This is clearly an undesirable result. Additionally, regulating the use of free public terminals provided by libraries presents some unique privacy and First Amendment implications not applicable to the other types of public terminals, which might further mitigate against application of the credentialing program discussed in this article.[101]

Weighing the benefits gained by the use of a credentialing system for free public terminal usage against the additional administrative costs borne by the proprietors of these terminals, and the potential loss of those terminals to the public, it seems that entities offering free, and presumably unmonitored, public terminal usage, such as libraries, might need to be exempted, at least initially, from such requirement. In order to bridge the "digital divide," public policy should act to encourage entities to offer free public terminals.[102] This is especially true with regard to the public library system, whose very existence is dedicated to the proposition that "[b]ooks and other library resources should be provided for the interests, information, and enlightenment of all people of the community the library serves."[103] Nonetheless, there may be other options for dealing with the use of free public terminals provided by libraries, which Congress may wish to explore at the time it considers implementation of a credentialing program.

Other institutions, such as high schools and universities, also offer free public terminals. Would it make sense to exempt them from this credentialing program as well? The most logical answer is that high schools and universities would not even fall within the purview of the proposed program since they are neither commercial nor are they available to the general public. Schools and universities usually have controlled access to their computer equipment, making them available only to registered students and faculty; a limited population.[104] Additionally, problems encountered by law enforcement when trying to trace virtual footprints back to a computer terminal are avoided because schools would likely already have many of the records law enforcement might seek; namely, records pertaining to students and faculty.

Of course, one could argue that because students pay for school, terminal usage is being "sold" to the public (i.e., the students) and could therefore

---

[100] *Id.* at 385 (referring to the discrepancy of Internet access across certain social lines as the "digital divide").

[101] A discussion of the potential First Amendment issues pertaining to public terminal use in non-commercial, public places, such as libraries, is beyond the scope of this article.

[102] *See* First & Hart, *supra* note 83, at 385.

[103] American Library Association, *Library Bill of Rights*, *available at* http://www.ala.org/work/freedom/lbr.html (Jan. 23, 1996).

[104] *See, e.g.*, Rosenberg v. Rectors and Visitors of the Univ. of Va., 515 U.S. 819, 823 (1995) (illustrating that the University of Virginia requires leaders of student organizations to be registered full time students in order to have access to the computing facilities).

qualify as commercial public terminals. This argument is unconvincing, however, because the primary reason that schools make these terminals available to students is to facilitate learning, not merely for the sake of Internet access.[105] Thus, because the offering of these terminals is so distinct from the reason for which the students pay to attend school, these terminals should not be deemed commercial public terminals. Additionally, if institutions made their computer terminals available to the general public (e.g., by holding a free Internet surf night for the general public) but did not charge for that usage, this would then fall into the category of free public terminals, such as those offered by libraries, for which credentialing may not be mandatory.

C. Free Public Terminals with an Underlying Commercial Motivation

The concept of credentialing becomes more complicated with regard to commercial establishments, such as coffeehouses, that provide free public terminals. While cyber-cafés and Kinko's facilities are easy to fit within the realm of operators of commercial public terminals,[106] because they directly charge for public terminal usage, the line between "commercial" and "free" becomes obfuscated when coffeehouses sell coffee and snacks while offering ostensibly "free" Internet access to customers.[107] For such establishments, although the main business purpose is to sell food and beverages, the public terminals offered act as an inducement or amenity for customers.[108] Since these public terminals are ostensibly offered to the public for free, these establishments probably do not engage in extensive monitoring. At the same time, however, the term "free" is somewhat deceptive because there is a commercial motive behind offering the use of these public terminals. Unlike the public library, public terminals offered at coffeehouses such as Starbucks are offered to encourage individuals to patronize these establishments and

---

[105] *See* Lisa Guernsey, *For the New College B.M.O.C., 'M' Is for Machine*, N.Y. TIMES, Aug. 10, 2000, at D7 ("The computer has . . . become the portal through which students do everything they need to do on campus.").

[106] *See* KINKOS.COM, *Our Services: Email Access/Internet/Telnet*, *at* http://www.kinkos.com/our_services/store_services/email.php (last visited Oct. 24, 2002).

[107] *See, e.g.*, STARBUCKS.COM, *High Speed Wireless Internet Access at Starbucks*, *available at* http://www.starbucks.com/retail/wireless.asp (last visited Nov. 7, 2002) (example of coffeehouse that offers Internet access as an inducement to engage in a commercial transaction).

[108] Of course, in the case of a Kinko's, the primary business began as copying and reproduction services. Nonetheless, public terminals for computer and Internet access is a natural corollary to Kinko's other service offerings, and can thus be said to have become one of Kinko's specific service offerings. In the case of a coffeehouse, by contrast, public terminals are clearly ancillary to the primary business model, which is to serve beverages and food to patrons, and are provided only to induce customers to engage in commercial transactions.

purchase drinks or food.[109] Indeed, these establishments generally post policies stating that these "free" public terminals are meant only for paying customers.[110]

To resolve this issue, we return to the two primary factors to consider when deciding whether a credentialing program should cover entities offering public terminals. First, we must consider whether the program would create an unreasonable administrative or monetary burden on the entity. Second, we must consider whether such a program would deter the offering of free terminals to the public. With regard to the first factor, it appears that the implementation of a credentialing program would not create an unreasonable administrative or monetary burden on coffeehouses. Coffeehouse customers must necessarily communicate with the proprietor to order their food and beverages and to pay for those products. This presents a viable opportunity to credential customers who wish to use public terminals. Indeed, coffeehouses often use such methods to control access to the restrooms on the premises. As such, they could use a similar system to enforce their "customers only" standard for public terminals. Thus, a credentialing program does not appear to create a heavy additional administrative burden on coffeehouses. Moreover, because the staff already employed by the coffeehouse could perform this credentialing, implementation of the program would likely not necessitate a large additional monetary outlay.

The second factor—the goal of not discouraging entities from offering free public terminals—likewise does not appear to be a great concern to these types of coffeehouses. Akin to the entities that offer commercial public terminals, there is a strong business incentive for coffeehouses to continue to offer free public terminals even if they must comply with the requirements of a credentialing program. While some coffeehouses may eliminate their free terminals due to the additional burden, a majority of the coffeehouses would likely continue to offer these free terminals to entice and encourage those customers to stay longer and make additional purchases.[111]

Another category of free public terminals, similar to those offered by coffeehouses, consists of public terminals available in hotel lobbies, airports, and stadiums.[112] While the coffeehouse offers public terminals as a means to

---

[109] *See* STARBUCKS.COM, *supra* note 107 ("The . . . service at Starbucks gives you the speed you need to quickly and easily check your e-mail, download that file you need for your next meeting, surf the Web, and get work done in coffeehouse comfort.").

[110] *See, e.g.*, HOTWIRECOFFEE.COM, *Hotwire Coffeehouse Homepage*, http://www.hotwirecoffee.com (last visited Nov. 7, 2002) (coffeehouse offering 15 minutes of free Internet access with each purchase).

[111] *See* Barrett, *supra* note 91, at 23.

[112] *See, e.g.*, Joie de Vivre Hospitality, *Maxwell Hotel Homepage*, http://www.jdvhospitality.com/hotels/sf_maxwell.html (last visited Nov. 8, 2002) (example of hotel offering Internet service in lobby); Craig Matsumoto & Terry Costlow, *Buy Me*

induce, or at least encourage, a commercial transaction, the terminal in the hotel lobby is not generally offered to induce a commercial transaction. Specifically, a person may choose to visit a coffeehouse in part due to a desire to surf the Internet. The free public terminal serves to draw in business and encourage commercial transactions. In such an instance, the free public terminal is more closely linked with a commercial transaction and should thus be treated similarly to commercial public terminals.

By contrast, it is unlikely that a person would choose to stay at a hotel for the express reason that the hotel offers a free public terminal in the lobby. Indeed, free public terminals would be just one of many amenities offered to guests. Hotels are more often chosen by price, location and service; not by a single amenity.[113] In fact, since many hotel guests can gain Internet access through their rooms, or through a business center in the hotel, it is unlikely that guests would incorporate the availability of free public terminals in their decision making process in deciding which hotel to patronize. Thus, in considering whether a credentialing program should exempt from coverage ostensibly free public terminals, we must ask whether the entity offering free public terminals does encourage a commercial transaction with the user of that terminal. In the case of a public terminal in a hotel or an airport, the answer is probably no.

D. Free Standing Public Terminals

One type of public terminal that warrants special mention is the free-standing, self-contained public terminal. This type of terminal is designed to operate much like a vending machine, without supervision or oversight, aside from routine testing or the occasional maintenance call (hereinafter referred to as "free-standing commercial public terminals"). As users must pay to use these terminals, these types of public terminals are best grouped with commercial public terminals. Unlike other commercial public terminals, however, these free-standing commercial public terminals are designed to be free of monitoring, and these terminals are generally not close in proximity to anyone who could perform such monitoring. These terminals are strategically located in high-traffic public areas, and left to the public without owner intervention. In this regard, the terminals are similar to a cigarette machine or

---

Some Peanuts and Processors, ELECTRONIC ENGINEERING TIMES, Apr. 5, 1999; SkyGuide, *Airport Internet Access: Cyber Stations for Travelers on the Run* (listing airports offering freestanding Internet kiosks, some of which offer free service funded by banner advertising), *available at* http://www.skyguide.net/ reference/internet.html (last visited Jan. 28, 2003).

[113] *See Study Shows Service Still Stands Supreme*, 16 HOTEL & MOTEL MANAGEMENT 212 (Sept. 15, 1997). Of course, while the purpose of offering public terminals in a hotel lobby may be to familiarize potential customers with the hotel and its amenities, the connection is much too tenuous to constitute an imminent commercial transaction, as opposed to the imminent transactions encouraged by offering public terminals at a coffeehouse.

a machine that dispenses candy.[114] For such terminals, establishing a credentialing program seems difficult, if not impossible, in part because monitoring these terminals runs counter to their free-standing, public purpose.[115]

Here, we return again to the two-factor analysis. The first factor, the additional administrative and monetary burden of implementing a credentialing program, tends to weigh heavily against the use of such a program with free-standing commercial public terminals. From an administrative point of view, as these terminals are designed to be free of oversight or monitoring, credentialing obfuscates the very purpose for which these terminals exist. Unlike the establishments that offer commercial public terminals discussed earlier, no staffing is present at or near these terminals. Hence, a credentialing program would require the heavy monetary burden of hiring new staff for the terminals.

Implementing a credentialing program entails many competing considerations with regard to the second factor—the goal of not discouraging entities from offering free public terminals. First, since these free-standing commercial public terminals are intended to be left unsupervised and unmonitored (thereby justifying the low charges for use and the commercial incentive to make these available), any program that requires credentialing and monitoring of these terminals would take away the very reason for which these terminals exist. This would likely lead to the removal of them from the public, which is contrary to a public policy favoring greater accessibility to the Internet.

At first glance, the two-pronged analysis of this article seems to point to the conclusion that these terminals should be exempt from the credentialing program. At the same time, however, such a result seems unfair because this would punish commercial establishments that have some type of pre-existing monitoring capability over those that have no such capability. Moreover, exempting free-standing commercial public terminals from the credentialing program would encourage the proliferation of these types of terminals and their use by criminals. This would likely exacerbate the very problems we are trying to eliminate: identifying users of public terminals.

Arguably, there may be other ways to deal with this problem. Perhaps these terminals could be required to follow a different type of credentialing procedure. For example, these terminals could have built in cameras, similar to Automated Teller Machines, which photograph terminal users. Alternatively, the machines could link the use of a credit card with a period of

---

[114] *See, e.g.*, American Terminal Public Internet Business Opportunities Franchise, *at* http://www.100franchises.com/american_terminal_public_internet_business_opportunities_franchise.htm (last visited Jan. 2, 2003) (example of business that sells free standing public internet terminals).

[115] *See id.*

terminal usage, thereby creating a record that identifies a criminal's virtual footprints.

These difficulties display the need for flexibility within any credentialing program. Regardless of how we resolve the problems presented by the various categories of public terminals, however, it is important that we craft a mechanism that takes into consideration each of these categories when developing a credentialing program.

E. Toward Developing a General Set of Guidelines

Using the two-factor analysis identified earlier, we can now construct a general set of guidelines for defining a credentialing program. First, a credentialing program should cover entities offering commercial public terminals because the additional administrative and monetary burden that it would incur would be manageable. Further, it is unlikely that the implementation of such a program would prevent businesses from continuing to offer those terminals to the public.

Conversely, the credentialing program might consider exempting, at least initially, entities that offer purely free public terminals without any monetary or other compensatory motive. This exemption would include public institutions that offer free public terminals, such as libraries, as well as free public terminals made available in airports and hotel lobbies.[116]

At the same time, a credentialing requirement should not exempt establishments where free public terminals are available as an inducement to an imminent commercial transaction (such as the purchase of beverages in a coffeehouse). This distinction comes from the reality that these free public terminals are offered to stimulate a commercial transaction with the user.

An argument that may be raised in response to the suggestion that a credentialing program should cover only commercial public terminals, and exempt truly free public terminals, is that such a program would redirect where and how the criminal element accesses the Internet. While this is a possibility, it is unlikely to be a large factor because, practically speaking, there are few free public terminals available. In addition to libraries, there occasionally may be a public terminal in a hotel lobby or an airport. However, the great majority of public terminals are commercial public terminals. Thus, from a purely practical standpoint, criminals will still necessarily use commercial public terminals. Moreover, as discussed previously, there may be other options for dealing with the use of these free public terminals, other than a blanket exemption, which would hopefully create a deterrent to the use of these free public terminals in the commission of Internet crime.[117]

Additionally, many criminals would still likely use commercial public terminals to commit their crimes for a number of reasons. First, the

---

[116] *See* discussion *supra* Part VI.B.

[117] *Id.*

credentialing program does not involve monitoring of a user's activities, and thus criminals who commit crime over the Internet may still believe themselves to be concealed by the Internet's anonymity and the use of shell accounts.

It is also feasible that a criminal might try to avoid detection as a result of being credentialed by presenting fake identification to the proprietor of the establishment. This would provide the criminal with an additional layer of comfort, believing his true identity to be concealed by the fraudulent document. Although the use of fake credentials would present an additional obstacle to tracing the identity of the user, at the very least law enforcement would have a picture of the suspect from which to conduct further investigation (since a proprietor would be responsible for matching the picture on the identification to the face of the person seeking to use the terminal). This would, in turn, avoid the investigative dead-end that often results today when tracing virtual footprints back to commercial public terminals. For example, the law enforcement agency could show the photograph to others in the community who may have seen the suspect and may be able to identify him. The law enforcement agency may also examine a copy of the fake identification to ascertain its origin, and then secure the identification of the suspect from the person who created the fake identification. In either case, the credentialing program would facilitate law enforcement investigations and provide law enforcement with yet another tool in its arsenal for fighting Internet crime.

VII. RESOLVING THE PROBLEM BY LEGISLATION

A. Prior Attempts to Implement Credentialing as a Means of Combating Crime—The U.S. Postal Service Experience

The problems presented by public terminals are similar to those faced by the United States Postal Service a few years ago as individuals were using commercial mail receiving agencies ("CMRA"), "drop boxes" in law enforcement lingo, for criminal activity.[118] CMRAs, such as Mail Boxes, Etc. outlets, provide an alternative to the use of post office boxes when an individual does not wish to receive mail at her place of residence or business.[119] As with the Internet, CMRA boxes provide a certain level of

---

[118] *See, e.g.*, U.S. Gen. Accounting Office Testimony, Health Care Fraud: Schemes to Defraud Medicare, Medicaid, and Private Health Care Insurers (July 25, 2000), *available at* http://www.gao.gov/new.items/os00015t.pdf.

[119] *See, e.g.*, MAIL BOXES, ETC., *Mail Boxes, Etc. Web Site*, http://www.mbe.com/ps/ms.html (last visited Jan. 2, 2003) ("MBE [Mail Boxes, Etc.] offers customers secure 24-hour access to mail and postal deliveries. When you get an MBE mailbox, you not only receive a private mailing address, access to delivery of large packages, 24-hour access to your mailbox, but also peace-of-mind. With an MBE mailbox, you no longer have to wait at

anonymity and privacy for the individual user.[120] Unfortunately, CMRA boxes and the Internet also share another, less auspicious similarity in that they both provide criminals with a level of anonymity that they can exploit when engaging in illegal conduct.

In an effort to deter the use of CMRAs for illegal purposes, and to enable law enforcement to track individuals using CMRA boxes for those illegal purposes, the Postal Service implemented new regulations in 1999.[121] These regulations require CMRAs to verify the identification of individuals registering to rent a CMRA box.[122] Specifically, in order to rent a box from a CMRA, an addressee:

> [m]ust furnish two items of valid identification; one item must contain a photograph of the addressee. The following are examples of acceptable identification: (1) [v]alid driver's license. (2) [a]rmed forces, government, or recognized corporate identification card. (3) [p]assport or alien registration card. (4) [o]ther credential showing the applicant's signature and a serial number or similar information that is traceable to the bearer. The CMRA owner or managers may retain a photocopy of the identification for verification purposes. The CMRA owner or manager must list the two types of identification . . . and write the complete CMRA delivery address used to deliver mail to the addressee . . . on Form 1583 [a form which must be maintained by the CMRA].[123]

The comments provided by proprietors of establishments offering public terminals, as well as by privacy advocates opposing the new CMRA regulations, were characteristic of their interests.[124] For example, some commentators argued that the new regulations would impose additional and unnecessary burdens on CMRAs, thus treating innocent entities as potential suspects.[125] In response, the Postal Service conceded that:

> [c]ompliance with the prescribed procedures may, as noted by some

---

home for a package delivery or risk having valuable shipments left on your doorstep. MBE can receive packages from any carrier and hold them in a secure location for pick-up at your convenience. Mailbox services are provided at every MBE location worldwide. Additional services include mail forwarding, fax receiving and the ability to call-in and check for new mail.").

[120] *See* Jere W. Glover, U.S. Small Business Administration: Office of Advocacy, Letter to Postmaster General, *at* http://www.sba.gov/advo/laws/comments/ps99_0625.html (June 25, 1999) (discussing CMRA industry and customers).

[121] Delivery of Mail to Commercial Mail Receiving Agencies, 64 Fed. Reg. 14,385 (Mar. 25, 1999) (to be codified at 39 C.F.R. part 111).

[122] *Id*. *See also* Anonymous, U.S. Postal Service CMRA Reg. Puts Survivors of Domestic Abuse in Danger, *available at* http://www.postalwatch.org/domestic.htm (May 28, 1999).

[123] 64 Fed. Reg. at 14,390.

[124] *See id*. at 14385-86.

[125] *See id*.

> commenters, impose additional burden on some CMRAs. It is true that CMRAs and their customers are, in the overwhelming majority of cases, innocent of any wrongdoing. Indeed, one commenter who supported the rule referred to CMRAs as 'unwitting conduits' in these frauds . . . where innocent people suffer inconveniences or expense due to the actions of a few lawbreakers.[126]

Commentators also opined that the identification requirements would "reduce the number of persons who use a CMRA address."[127] This commentary is not unlike the argument that privacy advocates foreseeably could raise in response to a proposal requiring implementation of a credentialing program for the use of public terminals; namely, that such a program would dissuade people from using these terminals to surf the Internet.

Despite the concerns raised by commentators, the Postal Service felt that the rules were a necessary step to prevent the types of crime for which the drop boxes had been used.[128] The Postal Service astutely noted that the new regulations did not place an onerous financial or administrative burden on CMRAs, but rather that "[t]he proposal simply requires that the CMRA match the information on the application with that on the valid identification presented."[129] Likewise, the credentialing program proposed in this article would require that proprietors of establishments offering public terminals covered by the program request a valid identification before providing a user with access, and retain, for a specified amount of time, a record of that user's name, and the specific computer used. This will, in turn, create a paper trail for law enforcement to follow when public terminals are used to commit cyber-crime.

While the postal regulations are a good beginning point for discussion, however, there is an important difference between requiring the presentation of identification for the use of CMRAs and requiring the presentation of that identification for the use of public terminals. Specifically, since CMRAs are used only to receive mail, and not to send mail, any regulation requiring identification as a pre-requisite to using a CMRA would presumably impact only the receipt of mail. In other words, if one were to look at the identification requirement as a theoretical limitation on the ability of an individual to maintain anonymity, such limit on anonymity would apply only to the receipt of mail as CMRAs are not used to send mail.

By contrast, the photo identification required as a pre-requisite for using a public terminal would affect a person's ability to both send and receive electronic mail in anonymity, as long as the sending or receiving of e-mail is performed from that public terminal. As discussed in the following section on

---

[126] *Id*.

[127] *Id*. at 14386.

[128] *Id*.

[129] *Id*.

privacy, however, the impact that a credentialing program would have on a person's ability to send and receive e-mail in anonymity is somewhat muted. This is due to the fact that the photo identification requirement in no way implies that we will monitor a user's activities while online, nor does it imply the collection of cookies, the review of e-mail, or tracking of the Web sites which a user visits. This proposal relies upon credentialing only as a means of identifying the individual who used a certain computer terminal on a given date and time. In short, the photo identification would not in any way permit a provider of public terminals to ascertain what the user did while online. Therefore, this credentialing program would not impact the anonymity of that user's activities while on a public terminal.

Lastly, as noted in the comments on the Postal Service regulation, "[t]he Postal Service strongly believes that full compliance with procedures outlined in the proposed rule and due diligence by the CMRA owners will be sufficient to deter wrongdoing."[130] Based upon the growing use of public terminals to commit Internet crime, and the inability of law enforcement to solve these crimes and identify the perpetrators without the requisite evidence, that sentiment could equally apply to the implementation of the credentialing program proposed by this article.

B. Prior Attempts to Implement Credentialing as a Means of Combating Crime –The Department of the Treasury and the SEC Experience

Implementation of a credentialing program as a means of deterring crime before it occurs and identifying and tracing criminals after a crime occurs is not a new concept. In fact, these types of requirements have become all the more common after the terrorist attacks of September 11, 2001. Pursuant to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act, these requirements have even become mandatory in some areas, thereby recognizing that crime is sometimes facilitated through a failure to properly credential individuals.[131]

For example, the Department of the Treasury, with the Securities and Exchange Commission ("SEC"), recently released the "Proposed Rule on Customer Identification Programs for Broker-Dealers."[132] Specifically, the proposed rule amends section 326 of the USA PATRIOT Act, which currently requires "broker-dealers to implement and comply with 'reasonable procedures' for: verifying the identity of customers 'to the extent reasonable

---

[130] 64 Fed. Reg. at 14386.

[131] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

[132] U.S. Sec. & Exch. Comm'n, Release No. 34-46192, File No. S7-25-02, *available at* http://www.sec.gov/rules/proposed/34-46192.htm (July 15, 2002).

and practicable;' maintaining records associated with such verification; and consulting lists of known terrorist."[133] The professed goal behind the implementation of Section 326 was to "facilitate the prevention, detection, and prosecution of international money laundering and the financing of terrorism."[134] The proposed solution by the Department of the Treasury and the SEC furthers this goal by adding regulations, including the requirement that broker-dealers registered with the SEC as a broker or a dealer (except for broker-dealers of security futures products) develop and implement a customer identification program ("CIP").[135]

In implementing the customer identification program, the Department of the Treasury and the SEC recommended the verification of customer identification through either documentary or non-documentary methods.[136] With regard to documentary evidence, a customer's identification may be verified through an "unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard," such as a driver's license or passport.[137] The CIP also provides for verification through non-documentary means, such as "obtaining a financial statement [or] comparing the identifying information provided by the customer against fraud and bad check databases."[138] Such procedures, however, would not be applicable, nor practical, with regard to the credentialing of users of public terminals due to the short-term, transient nature of such usage.

Conversely, because the credentialing program would not be encumbered by many of the banking and financing laws applicable to the Department of the Treasury's and the SEC's proposed rule, the credentialing program could include additional methods for verifying user identity not available under the CIP.[139] This would, in turn, help avoid any discriminatory impact a credentialing program might have on those people who may not have a government-issued identification, by permitting the use of non-government-issued identification such as photo credit cards. It is also worthwhile to note that, unlike the government's proposed program, proprietors of public terminals would not have to undertake steps to verify the accuracy of the identifying information provided aside from ensuring that the face on the

---

[133] *Id.*

[134] *Id.*

[135] *See id.*

[136] *See id.*

[137] *See id.*

[138] *See id.*

[139] *See, e.g.*, VISA, *Protect Your Visa Card Online with a Personal Password*, http://www.usa.visa.com/personal/secure_with_visa/verified_by_visa.html (last visited Jan. 31, 2003) (describing how Visa cardholders can protect against online credit fraud by using a personal password).

identification matched the face of the user presenting the identification.[140]

Another similarity between the credentialing program recommended by this article and the CIP is the record-keeping requirement. Pursuant to the CIP, broker-dealers

> [m]ust maintain copies of any documents that were relied upon . . . evidencing the type of document and any identification number it may contain. For example, if a customer produces a driver's license, the broker-dealer must make a copy of the driver's license that clearly indicates it is a driver's license and legibly depicts any identification number on the license.[141]

Similarly, the credentialing program would require proprietors of public terminals to make a copy of the photo identification provided by perspective public terminal users so that this information could be furnished to law enforcement when necessary. Unlike the government's CIP, however, which requires broker-dealers to maintain all records of customer identity verification for "five years after the date the account [in question] is closed or the grant of authority to effect transactions with respect to an account is revoked,"[142] such record retention requirements could be substantially shorter for the proprietors of public terminals. To determine what would constitute a reasonable period of time for retention of these credentialing records will require a careful balancing between the burden on proprietors of maintaining these records and the needs of law enforcement. Furthermore, due consideration must be given to the potential time window within which law enforcement would likely be seeking production of these records.

While the government's proposed CIP may pertain to investing activity, and may not have precisely the same goals as the credentialing program recommended by this article, both programs possess a similar policy objective; fighting crime and terrorism. Likewise, while the SEC's implementation of a customer identification program is a necessary and appropriate balance between privacy interests and security concerns,[143] one also could reasonably argue that a similar balance mitigates in favor of implementing a credentialing program for the use of public terminals. In both cases, law enforcement's ability to fight crime and terrorism is substantially furthered by the programs. Also, in both cases these programs benefit society in terms of increased safety and security.

---

[140] *See id.*

[141] *Id.*

[142] *Id.*

[143] *See, e.g.*, 147 Cong. Rec. S. 10547 (daily ed. Oct. 11, 2001) (Senator Leahy, among others, expresses his views on the importance of the USA PATRIOT Act in light of recent terrorist attacks).

C. Privacy Implications of a Legislative Solution

It has often been said that there is no such thing as absolute privacy, nor is there such a thing as absolute transparency. Yet, things are not nearly as futile as Scott McNealy, the chief executive officer of Sun Microsystems, Inc., observed when he stated "[y]ou have no privacy, get over it."[144] In today's information society, we often perform a balancing act between the privacy of individuals and the needs of businesses and government officials to access personal information. On the other hand, the adoption of a law requiring the capture of an individual's identification information before permitting an individual to use a public terminal does not necessarily amount to a loss of privacy. Mechanisms that assist responsible and robust law enforcement can actually protect and enhance the privacy enjoyed by our citizenry. For example, the ability to use the information secured through the credentialing program to apprehend and prosecute Internet criminals will deter the theft of personal information from credit card and credit agency databases,[145] will reduce the number of individuals who are the targets of identity theft,[146] and will lead to an overall drop in the victimization of the citizenry's privacy on the Internet.[147]

As such, the question should not be whether the proposed credentialing program will have privacy implications. Rather, the question becomes whether the program will yield a net loss in privacy—that is, whether the program will over-subordinate an individual's privacy to the needs of government officials to access personal information in order to perform their duties. Only if the answer to this first question is yes, do we proceed to the next question, which is whether this loss of privacy is worth the societal good (in this case, the apprehension and prosecution of criminals and terrorists) created as a result of the lost privacy.

Another consideration to bear in mind when assessing the privacy implications of the credentialing program is that in today's world many of us already surrender far more personal information on a daily basis, without any restriction on the use of that information, than that which would be required by the credentialing program. For example, supermarkets often offer customers frequent shopper cards that are swiped before a cashier rings up the purchases of that customer. As purchases are rung up, a computer checks the products against a list of specials offered to cardholders, and reduces prices accordingly. In performing this task, however, these computers are able to track every

---

[144] Ari Schwartz, *Privacy at the Crossroads*, FED. COMPUTER WK. (Mar. 12, 2001), *available at* http://www.fcw.com/fcw/articles/2001/0312/pol-schwart-03-12-01.asp.

[145] *See, e.g.*, Benjamin Weiser, *Identity Ring Said to Victimize 30,000*, N.Y. TIMES, Nov. 26, 2002, at A1 (showing how widespread and serious identity thrft casea have become).

[146] *See id.*

[147] *See, e.g.*, Robert Hanley, *Former H&R Block Manager Accused in Identity-Theft Ring*, N.Y. TIMES, Jan. 3, 2003, at B2.

product purchased by that customer and keep an ongoing list of these products, the product categories, and the preferred brand names, thereby enabling the assembly of a sophisticated profile of that customer.[148]

While privacy advocates may have concerns about the information provided through a credentialing program, the goal of which is to deter and prosecute Internet crime, personal information collected through this program is far less than the personal information provided to a store in order to receive discounted prices on products. In many ways, the credentialing program is less invasive of privacy rights than a frequent shoppers program because the credentialing program will not track the online sites visited by users, while grocery stores do in fact track comparable detailed information about the individual, such as purchases and preferred product brands.

Assuming, for arguments sake, that the credentialing program does lead to a net loss of privacy, the program should not sacrifice privacy interests any more than necessary to accomplish the specific goal for which the program is created. In other words, the program shall not permit proprietors of public terminals to use this identification information for activities such as marketing to customers or profiling customers for the purpose of spawning future commercial transactions. In essence, participation in the credentialing program would mean surrendering identification information for a very specific and narrowly tailored purpose and that information should not be used for anything other than to accomplish that purpose.

As such, any legislative implementation of a credentialing program should incorporate explicit privacy protections with appropriate sanctions. These protections should include prohibitions on the unauthorized use or disclosure of this information, as well as severe monetary penalties for the violation of those prohibitions. Specifically, the credentialing program should include a prohibition on: (i) the disclosure of this identification information to anyone other than law enforcement, including a prohibition on the sale of this information to third parties; (ii) the use of this information for purposes other than official law enforcement purposes, including a ban on the use of this information for marketing to, or profiling of, customers; and (iii) the de-identification or aggregation of identification information gathered through the credentialing program.[149] To preserve the privacy of public terminal users, the

---

[148] *See, e.g.*, Martin Sloane, *Frequent Shopper-Card Can Have a High Price*, UNITED FEATURE SYNDICATE, *available at* http://www.chron.com/content/chronicle/food/98/04/15/4-15-coupon.0-0.html (Apr. 10, 1998); Robert O'Harrow, Jr., *Bargains at a Price: Shoppers' Privacy*, WASH. POST, Dec. 1, 1998, at A1, *available at* http://www.geocities.com/ WallStreet/5395/clubcard/115l-123198-idx.html.

[149] Of course, in enacting a credentialing program, Congress may choose to permit proprietors of public terminals to utilize a type of opt-in or opt-out marketing agreement with public terminal users that would enable those proprietors to utilize the identification information for marketing purposes. Examples of this are already widely used on the

program should also require secure storage of the identification information provided through the credentialing program, such as a locked file cabinet, with access limited to need-based situations. Finally, stringent guidelines should be included in any legislation that requires the prompt destruction of this identification information once the specified amount of time has expired.[150]

VIII. RESOLVING THE PROBLEM BY SELF-REGULATION

A. The Benefits of Self-Regulation

While legislation offers one option for resolving the problem presented by criminal use of public terminals, a second option is to initiate a dialogue among the various businesses that provide public terminals in an effort to encourage and develop voluntary self-regulation. Such a dialogue would need to involve a cross-section of various businesses that the program would affect. This list would potentially include cyber-café chains, large office supply chains such as Kinko's and Staples, coffee chains such as Starbucks, as well as a host of smaller businesses. Due to the large variety of businesses that provide public terminals and the lack of established lobby groups (e.g., the Recording Industry Association of America or the Business Software Alliance in other contexts), undertaking such a dialogue would probably present a number of practical and tactical difficulties. Nonetheless, the need for such a dialogue is self-evident. Law enforcement must be able to identify criminal users of public terminals in order to deter the commission of such crimes and to apprehend those who engage in such crimes. Otherwise, it is likely that Internet crimes will increase in occurrence. Furthermore, if an act of cyber-terrorism results in a tragic loss, legislators may feel compelled to act unilaterally in order to satisfy the call for accountability and justice.

The possibility of opening a dialogue to permit businesses to volunteer a set of standards to resolve this problem is indeed quite appealing. On the positive side, this would likely result in a well-balanced solution that takes into account the administrative and monetary costs to businesses as well as the needs of law enforcement. Another benefit of this resolution is that businesses that offer public terminals would more readily and expediently adopt such an agreement. Additionally, because such a solution would have considered the needs of the businesses, as well as the associated costs and practicalities, implementation of this standard would most likely be easier, practically speaking, than a government-mandated standard. More importantly, as a program developed voluntarily by businesses, businesses and consumers would not view it with the same skepticism as a government-mandated program.

Finally, as discussed previously, a legislated credentialing program will

---

Internet.

[150] *Cf.* ECPA discussion, *supra* Part IV.

probably need to initially exempt proprietors that offer free public terminals so as not to impact or discourage the provision of such a vital service to the public.[151] If such a program developed through dialogue and voluntary self-regulation, however, it is feasible that proprietors of free public terminals could also be considered in designing the solution. At the very least, the dialogue by proprietors would be worthwhile in order to secure their input. In addition, it would be worthwhile to seek the input of the business community regarding alternative methods for securing the necessary credentialing information from users of free public terminals without the costs likely associated with a legislatively mandated credentialing program.

B. Drawbacks of Self-Regulation

Unfortunately, recent history has demonstrated that self-regulation is not always successful. One prime example is the implementation and posting of privacy policies by businesses on their Web sites. Beginning in 1995, the Federal Trade Commission ("FTC") called for businesses to implement and post clear and conspicuous privacy policies on their Web sites, advising people of what the FTC now refers to as its fair information practices.[152] These practices include notice, choice, access and security, and regulate how information may be collected by Web sites.[153] For a number of years leading up to the FTC's creation of these practices, the FTC repeatedly urged the Internet community to police its own use of personal information, having conducted numerous audits of various Web sites to determine the level of compliance with what it deemed acceptable privacy practices.[154] While businesses did make some attempts at self-regulation in the hopes of warding

---

[151] *See* Free Public Terminal discussion, *supra* Part VI.B-E.

[152] *See* FTC Privacy Report, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, *available at* http://www.ftc.gov/os/2000/05/testimonyprivacy.htm (May 25, 2000).

[153] *Id.* (explanation of the different fair use practices: "Notice—Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it, how they use it, how they provide Choice, Access, and Security to consumers"; "Choice—Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided. Such choice would encompass both internal secondary uses and external secondary uses"; "Access—Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review the information and to correct inaccuracies or delete information"; "Security—Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers").

[154] Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress*, (1999) (statement of Robert Pitofsky, Chairman of the FTC before the Subcommittee of Telecommunications, Trade, and Consumer Protection of the House Commerce Committee), *available at* http://www.ftc.gov/opa/1999/9907/report1999.htm.

off legislative intervention, these attempts were not wholly successful.[155]

In July 1999, the FTC released a report to Congress on the progress of industry self-regulation.[156] The FTC recognized in the report that (1) a number of notable industry responses had occurred in response to calls for self-regulation, including the proliferation of privacy organizations such as Truste (www.truste.com); and (2) the adoption of policing and complaint resolution requirements.[157] Yet even with that progress, self-regulation had not progressed so as to be deemed adequate. Nonetheless, the FTC conceded the responsibility of online privacy to the industry.

Less than a year after the FTC concluded that legislative intervention was unwarranted, however, the FTC reversed its position. In its report to Congress on May 22, 2000, the FTC recommended that Congress enact legislation "to empower the FTC to pass rules *requiring* Web sites to give notice of their information practices, to allow individuals to control how their data is used, to allow individuals to access and correct their data and to require security measures."[158] Even with the FTC's call for legislation, however, there remained a distinct lack of consensus on how best to deal with the need for better privacy protections online.[159]

If the implementation of acceptable privacy practices is any indication of the success of self-regulation, establishing a credentialing program through voluntary self-regulation could be a long and bumpy road. In some ways, self-regulation in this area could be even more difficult since it is not as clear who are the players necessary to begin a dialogue. Furthermore, the potential burdens on businesses when implementing these standards could be higher than they were with regard to online privacy standards and regulations. This is especially true when one considers the administrative and monetary costs that

---

[155] *See* Chris Oakes, *Study: Self-Policing a Failure* (June 22, 1998), *available at* http://www.wired.com/news/politics/0,1283,13173,00.html (documenting the failure of Web sites involved in the Internet economy to institute privacy practices). *See, e.g.*, *On the Web You Have No Secrets*, PC WORLD, July 1, 1999 (The Online Privacy Alliance, a group composed of more than 80 businesses, was launched in July 1998 to promote self-regulation as a solution to privacy concerns); Kenneth Neil Cukier, *Is There a Privacy Time Bomb*, RED HERRING, Sept. 1999, *available at* http://www.westlaw.com ("As a result of pressure from consumers and privacy advocates, the World Wide Web Consortium, a standards forum, has issued a draft specification called Platform for Privacy Preferences, or P3P.").

[156] *See* Self-Regulation and Privacy Online, *supra* note 155, at 9-12.

[157] *Id.*

[158] *See FTC Seeks Authority to Regulate Online Privacy*, TECH L.J., May 23, 2000, *available at* http://www.techlawjournal.com/privacy/20000523.htm. In issuing its Report, two of the five FTC Commissioners dissented.

[159] In a contrary view, some believe that self-regulation is inevitable because the ever-increasing value of this personal information will create an incentive for many companies to "husband the data like a trade secret rather than disseminate it to the highest bidder." *See* Cukier, *supra* note 155, at 2.

businesses would encounter in assessing a solution that will sufficiently enable law enforcement to track criminals who use public terminals. While the implementation and posting of clear and conspicuous privacy policies could have potentially impacted the way businesses used their customers' personal information, such a program would not have required the immediate outlay of cash that a credentialing program might; nor would it have required the assumption of a large additional administrative burden. A program designed to track users of public terminals, on the other hand, could involve a direct outlay of cash along with an immediate assumption of additional administrative duties. This would potentially give rise to even more reluctance amongst industry members to arrive at a consensus. Indeed, the monetary costs to the businesses affected by the credentialing program actually provide a disincentive to implement such a solution.

At the same time, however, the number of businesses included in such a dialogue is far less than the number implicated by the debate surrounding the online privacy policy issue. While the privacy policy issue affected any business with an Internet presence—large and small, foreign and domestic, regardless of the specific business model or product—a dialogue would include only those businesses that offer public terminals. Ideally, the fact that this group would potentially be smaller and more insular would hopefully expedite the progress of a self-regulatory dialogue.

One final concern with regard to a self-regulatory resolution pertains to the privacy implications of such a solution. If the credentialing program were implemented via legislation, such program would likely include certain privacy protections for the credentialing information provided by terminal users. Specifically, such protections would likely involve a prohibition on the use, sale or disclosure of such information for purposes other than furnishing such information to law enforcement engaged in a lawful investigation. Such protections may also include a prohibition on the linking of such information to other disparate pieces of information, thus creating dossiers of customers and using the information for purposes of customer aggregation.[160]

Self-regulation, by contrast, would not entail mandatory restrictions on the use of information secured from public terminal users, leaving the privacy protections afforded such information up to the discretion of the individual

---

[160] *See* Cukier, *supra* note 155, at 3 (quoting John Hagel III, a McKinsey & Co. principal and coauthor of Net Worth, "[t]he most valuable economic asset of these Internet businesses is the profiles—the ability to capture information about the customer and use it for economic purposes. The profile is really the core business assumption."); Matthew Kohel, *The Privacy Amendment (Private Sector) Bill 2000: The Australian Government's Substandard Attempt to Allay Privacy Concerns and Regulate Internet Privacy in the Private Sector*, 27 BROOK. J. INT'L. L. 703, 729 (2002) (small businesses freely pass information to one another in order to build up profiles of customers); Erica S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 No. 5 COMPUTER LAW 7, 10 (1999).

businesses gathering the information. This discretion could potentially lead to a patchwork of privacy standards and a lack of consistency in enforcement, which could in turn raise concerns with privacy advocates. While the best solution to this privacy problem would be for businesses to concurrently develop a set of applicable privacy standards, such selflessness on the part of business is unlikely.[161] Additionally, while self-regulation could promote privacy, only statutory law could mandate privacy protection.

Despite the foregoing issues, self-regulation remains a viable option for resolving the problem currently posed by the anonymous use of public terminals to commit acts of cyber-crime and cyber-terrorism.

IX. CONCLUSION

On the morning of September 11, 2001, for the second time in America's history, the nation awoke to an unprovoked surprise attack on its soil. The ensuing carnage, and the horrific pictures etched into our minds forever altered the perception of our safety and security at home. As a result of these attacks, people around the country reassessed their priorities, and in many cases agreed to forego some of their privacy in return for greater security. Likewise, Congress passed the USA PATRIOT Act in record time; an Act that provides law enforcement with important new tools to detect, investigate and obstruct potential acts of terrorism and other threats to our national security. As tragic as September 11th was for us all, however, we were fortunate that the damage caused by the attacks was not amplified through concurrent acts of cyber-terrorism, a term known as "swarming."[162] Yet, the distinct possibility of such attacks clearly exists. Imagine, if you will, how much greater the death toll in the World Trade Center attack might have been had the New York Police Department, the Fire Department of New York and the Port Authority Police not responded because the call for help never went out (i.e., if the terrorists had used the Internet to disable the communications network). Let us take an even less extreme example. To date, the damage caused by computer viruses has been primarily isolated to monetary losses by companies. Imagine a computer virus used to infect and disable the computer systems in a hospital, interfering with the normal operation of vital life-saving equipment, not to mention the ability of doctors to attend to their patients. Cyber-crime and cyber-terrorism pose just as much of a threat to the safety and security of Americans as their real-world counterparts.

While the PairGain case study presented in this article dealt with security fraud over the Internet, the Internet is regularly used to commit crimes with far graver consequences than securities fraud. Indeed, we have all read of the

---

[161] *See* FTC v. Toysmart.com, LLC, 2000 WL 1523287 (D. Mass. 2000).

[162] Chris Wallace, *U.S. Government Gearing Up for Cyber-Terrorism*, KOLO-TV NEWS (Sept. 14, 2002), *at* http://www.kolotv.com/money.php?link=readmore&sid=3131.

rampant rise in child pornography perpetrated over the Internet, as well as the all too often stories of young women lured to fatal meetings with strangers they met over the Internet. Everyone wants to see these crimes solved and the perpetrators caught. Yet, very few people—not private citizens, not legislators, and in many cases, not even law enforcement trained solely in real-world investigations—actually understand what is involved in catching these criminals.

There is little doubt that the types of record creation discussed in this article might very well implicate privacy.[163] However, because the records maintained pursuant to the credentialing program will identify a user of a resource on a given date, at a given time, and nothing more, the privacy interests are slight. There is no suggestion that we attempt to capture the actual Web sites visited by a user or how that user used the computer. In essence, the privacy implications of this recommendation are negligible, at worst, and the benefits are substantial. Conversely, if the perpetrator of a crime cannot be identified, the criminal cannot be apprehended. And if the criminal is not apprehended, the criminal will not be punished, thus denying justice to the victims of the crime and eliminating the deterrent effect of our criminal laws.

As Sherlock Holmes once observed, "[i]t's a wicked world, and when a clever man turns his brain to crime it is the worst of all."[164] While the Internet has opened up a whole new world of access to information and communication, it has also opened up a whole new wicked world of cyber-crime and cyber-terrorism to clever men and women around the globe. As the age old adage cautions, those who do not learn from history are doomed to repeat it. We must take the lessons of the terrorist attacks of September 11, 2001 to heart and apply it to all aspects of our lives, including enhancing the abilities of our law enforcement in the area of cyber-crime. Only through reasoned, proactive steps can we hope to fight this insidious new virtual evil, and avoid repeating the oversights that led to the terrorist attacks.

---

[163] *See* Privacy Implication discussion, *supra* Part VII.C.

[164] ARTHUR CONAN DOYLE, *The Adventure of the Speckled Band*, *in* ADVENTURES OF SHERLOCK HOLMES 165, 182 (Penguin Books 1986) (1892).