Stanford Technology Law Review

Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies

HARRY A. VALETK*

CITE AS: 2004 STAN. TECH. L. REV. 2
http://stlr.stanford.edu/STLR/Articles/04_STLR_2

"It has become appallingly clear that our technology has surpassed our humanity."
- Albert Einstein

¶1 On January 12, 2003, Brandon Vedas, a twenty-one-year-old computer expert from Arizona, died after taking a lethal dose of controlled substances.[1] Sad as it is to know that a troubled young man took his own life, the circumstances surrounding Brandon's apparent suicide offer a glimpse of a new and unfamiliar landscape. At the time of his death, Brandon had a captive audience, watching him through a webcam, as he ingested a lethal cocktail of drugs and alcohol in full view of a group of chat room companions. According to the chatroom transcript, some participants warned Brandon against taking too many drugs, while others actually encouraged him to take more. Brandon's last coherent words were "I told u [sic] I was hardcore."[2]

¶2 Whether or not Brandon's death was the result of undiagnosed depression, a reckless experiment gone awry, or simply an accident inspired by peer pressure remains uncertain. What his tragic death does establish, however, is the permanent impact that information and telecommunications technology (generally referred to as the "Internet") has had on the way we interact, and its power to creep into the most intimate spheres of our existence. For better or for worse, the Internet has transformed our social landscape, and if current trends hold true, we are at the cusp of a new era facing the dark sociopolitical policy concerns of an interconnected existence. For instance, figures show online dating is rapidly becoming a fixture of single life for more than 45 million adults of all ages, backgrounds, and interests.[3] Researchers at the University at Buffalo have developed a system that allows one person to experience the sense of touch felt by another, and transmit the sensation over the

* Harry A. Valetk, Trial Attorney, U.S. Department of Justice, Civil Division, New York City. Chief Legal Officer of Wiredsafety.org, Wiredpatrol.org, and Wiredkids.org. Adjunct professor at Bernard M. Baruch College, Zicklin School of Business, CUNY. J.D., 1998, Benjamin N. Cardozo School of Law, B.B.A., 1995, Bernard M. Baruch College, Zicklin School of Business, CUNY. My heartfelt thanks to the many talented professionals whose valuable input helped shape this final product. I would also like to give special thanks to Professor Peter Yu for his guidance, support, and penetrating insight. The opinions expressed in this article are the author's own, not those of the U.S. Government. The author may be reached by email at harry@valetk.com. His website is at www.valetk.com.

[1] *See Net Grief for Online Suicide*, BBC NEWS, WORLD EDITION, Feb. 4, 2003, *at* http://news.bbc.co.uk/2/hi/technology/2724819.stm (last visited Mar. 21, 2004).

[2] *Id.*

[3] *See* Amy Harmon, *Online Dating Sheds Its Stigma as Losers.com*, N.Y. TIMES, June 29, 2003, at A1. *See also*, Anna Mulrine, *Love.com*, U.S. NEWS & WORLD REP., Sept. 29, 2003, at 52 (reporting that hectic lifestyles, and revolutionary reforms in mating practices, have led 50% of American single adults to matchmaking websites).

Internet.[4] A 2003 study examining the media interests of young adults found that teens now spend more time on the Internet than watching television.[5] A report on e-mail at work found that 98% of users with Internet access use e-mail on the job.[6]

¶3 The Internet's awesome power of interconnectivity has made it by far the fastest growing medium in human history.[7] According to a 2002 report by the United Nations ("U.N.") Conference on Trade and Development, 655 million people around the world now have Internet access.[8] In India, Internet access increased 27.3% from 5.5 million users in 2000 to 7 million users in 2001.[9] During the same time period, Internet users in South Africa increased by 27.8%, in Brazil by 60%, and in Mexico by 34%.[10] A 2002 study by the U.S. Department of Commerce found that 143 million Americans (about 54% of the population) were using the Internet in September 2001—an increase of 26 million in thirteen months.[11]

¶4 But, with increased online integration also comes a new vehicle for misconduct. Operating at a tortured pace, the legal systems of the world have only now begun to recognize the realities of the Internet's unregulated, borderless realm. So far, only a patchwork of laws exists to protect users against emerging criminal conduct in cyberspace. According to published reports, only fifty or sixty countries have specific laws against cyber-crimes.[12] Interpol representatives estimate that more than a hundred countries have no laws on computer offences.[13] Unfortunately, gaping holes in the law, coupled with the Internet's global setting, create new vulnerabilities for the Internet community at large.

¶5 A joint report by the National White Collar Crime Center and the U.S. Federal Bureau of Investigation ("FBI") found that fraud complaints in the United States arising from Internet transactions tripled in 2002 relative to the year before.[14] The FBI's Internet Fraud Complaint Center received 48,252 complaints in 2002; in 2001, it only received 16,775 complaints.[15] The report also found that approximately 46% of the complaints involved auction fraud.[16] Not surprisingly, the total monetary loss tripled from $17 million in 2001 to $54 million in 2002.[17]

¶6 Still, the United States is not the only nation facing increased vulnerabilities in cyberspace. In the United Kingdom, law enforcement officials have found that cyber-crime

---

[4] *See* Daithí Ó. hAnluain, *Reaching Through the Net to Touch*, WIRED NEWS, July 3, 2003, *at* http://www.wired.com/news/technology/0,1282,59462,00.html (last visited Mar. 21, 2004).

[5] *Youth spend more time on Web than TV*, FORBES.COM, July 24, 2003, *at* http://www.forbes.com/technology/newswire/2003/07/24/rtr1037488.html (last visited Mar. 21, 2004).

[6] DEBORAH FALLOWS, PEW INTERNET & AMERICAN LIFE PROJECT, EMAIL AT WORK (2002), *available at* http://www.pewinternet.org/reports/toc.asp?Report=79 (last visited Mar. 21, 2004).

[7] *See* Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J. LEGAL COMMENT. 393, 394 (2002).

[8] U.N. CONF. ON TRADE AND DEV., E-COMMERCE AND DEVELOPMENT REPORT ix, U.N. Doc. UNCTAD/SDTE/ECB/2 (2002), *available at* http://r0.unctad.org/ecommerce/ecommerce_en/edr02_en.htm (last visited Mar. 21, 2004).

[9] *Id.* at 4.

[10] *Id.*

[11] U.S. DEP'T OF COMMERCE, ECONS., AND STATISTICS ADMIN., NAT'L TELECOMMS. AND INFO. ADMIN., A NATION ONLINE: HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET (2002), *available at* http://www.ntia.doc.gov/ntiahome/dn/ (last visited Mar. 21, 2004).

[12] Kim Yeon-hee, *World Crime Experts See Need for Laws, Ties*, INFOWORLD, Oct. 16, 2002, *at* http://www.landfield.com/isn/mail-archive/2002/Oct/0068.html (last visited Mar. 21, 2004).

[13] *Id.*

[14] *See* INTERNET FRAUD COMPLAINT CTR., NAT'L WHITE COLLAR CRIME CTR. AND F.B.I., IFCC 2002 INTERNET FRAUD REPORT 4-5 (2003), *available at* http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf (last visited Mar. 21, 2004) (noting that although a small portion of the referred complaints involved non-Internet-related fraud, more than 90% of referrals involved fraud committed over the Internet).

[15] *See id.* at 6.

[16] *Id.*

[17] *Id.*

incidents are doubling every eighteen months.[18] In South Korea, the National Policy Agency reported that in 2001 cyber-offences shot up 126% from the year before, to 33,289 cases, and totaled 39,482 cases in the first eight months of 2002.[19]

¶7 Equally unsettling is the societal impact of criminal activity that goes beyond quantifiable figures. Although the ongoing developments in the Internet's potential hold a special promise for our future, the global presence of this new medium has introduced a host of new dangers that transcend cultural norms, national boundaries, and traditional territorial law enforcement mechanisms.

¶8 Benefiting from the confusion, many cyber-predators exploit gaps in the law, test its limits, and hide behind conflicting definitions of criminal activity. Identity predators, for example, abuse lax information-sharing policies to commit identity fraud. Cyberstalkers track their victims online, sending offensive e-mails or menacing messages using Instant Messaging technology. Spammers not only bombard users with unsolicited junk e-mail, but can also spread destructive computer viruses—like the SoBig.F virus—within messages that have misleading subject lines.[20]

¶9 In a June 2003 message to WiredSafety.org,[21] one cybercrime victim aptly summarized the user frustrations of an expanding, but loosely-regulated, virtual realm:

> *I am being harassed, stalked, and my personal identity has been plastered over the Internet on a home business web page. I have contacted the Sheriff's department, but it does not involve a large amount of money. . . . Is there anyone out there that can give me some advice?*[22]

¶10 This article will strive to shed light on the dark arts of cyberspace by examining three Internet safety policy concerns that remain largely overlooked in this virtual realm: identity theft, cyberstalking, and informational privacy invasions. Part I will discuss the gravity of the identity theft situation in the United States in light of Corporate America's promiscuous use of the Social Security Number ("SSN") as the primary method of identifying individuals. Part II will discuss the emerging social concerns in cyberspace involving harassment, bullying, and other scare-tactics known as cyberstalking. Part III will touch on the role informational privacy invasions play in promoting criminal activity in cyberspace. Part IV will lay out the policy challenges that lie ahead, given the rapid integration of Internet technology into the fabric of our everyday lives. In sum, this article will press the need for sound Internet policies that foster economic prosperity and secure a reasonable sense of personal safety.

I. IDENTITY THEFT AND SOCIAL SECURITY NUMBER MISUSE

¶11 To be sure, identity theft is not a new crime. In fact, history can trace varying forms of identity theft—like forging checks or impersonating credit-worthy buyers—back for centuries.[23] But, thanks to the Internet's endless resources, the opportunity to commit identity fraud is everywhere. Seizing this opportunity in new ways every day, savvy criminals

---

[18] Robert Jaques, *High-tech Crime Follows Moore's Law*, VNUNET.COM, June 27, 2003, *at* http://www.vnunet.com/News/1141886 (last visited Mar. 21, 2004).
[19] *See* Yeon-hee, *supra* note 12.
[20] *See Spammer blamed for SoBig.F virus*, CNN.COM: TECHNOLOGY, Aug. 22, 2003, *at* http://www.cnn.com/2003/TECH/internet/08/22/sobig.culprit (last visited Mar. 21, 2004).
[21] WiredSafety.org is an Internet safety, help, and education organization. Wiredsafety.org is a 501(c)(3) non-profit corporation run entirely by volunteers worldwide. More information is available at http://www.wiredsafety.org.
[22] E-mail sent to LegalEagles at WiredPatrol.org (June 16, 2003) (on file with author).
[23] *See* Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 354 (2003).

are now far more capable of getting confidential personal information, and using it to commit fraud.

¶12 Highlighting just how vulnerable consumers are, a consumer advocacy group in October 2003 skywrote the first five digits of the SSN of Charles Prince, Citibank's chief executive officer, in New York City.[24] The same group also purchased the SSNs of Attorney General John Ashcroft, Central Intelligence Agency ("CIA") director George Tenet, and Federal Trade Commission ("FTC") chairman Timothy Muris on the Internet for just $30 each. In July 2003, the FTC warned consumers about "phishing" scams. "Phishing" occurs when identity predators send official-looking messages stating that, due to technical system problems, recipients should forward or resubmit credit card information, SSNs, or other key identifying data. To fool victims, "phishers" create pages using information from legitimate websites. According to FTC chairman Timothy Muris, "phishing" is a two-fold scam: "Phishers first steal a company's identity and then use it to victimize consumers by stealing their credit identities."[25] Among those targeted by these "phishing" scams in 2003 were companies like Best Buy, UPS, Bank of America, PayPal, and First Union Bank.[26] Finally, in February 2003, Monster.com, the most popular Internet job board, warned users about an increasing number of false job postings used to illegally collect personal information from unsuspecting job seekers.[27]

¶13 Simply stated, identity theft occurs when a thief obtains confidential information about another individual, and uses it to defraud others. The most dangerous, and fairly common, form of identity theft is "true name fraud," which occurs when an imposter opens a new credit account in the victim's name.[28] By contrast, "account takeover" involves instances in which an imposter uses an existing credit account to make fraudulent purchases.[29]

¶14 What makes identity theft so alluring to criminals is its low-risk, faceless, and lucrative nature.[30] These features explain why identity theft today ranks among the fastest growing white collar crimes, victimizing millions of consumers in new ways every year. According to a September 2003 study by the FTC, approximately 10 million consumers fell victim to some form of identity theft within the past year.[31] At this pace, some experts predict that one in four Americans will fall victim to identity theft at some point in their lives.[32]

¶15 Identity theft is uniquely dangerous because it is an enabling crime—one that permits criminals to commit other crimes. Identity predators have used the names of their victims to rent apartments, obtain employment, subscribe to online pornographic services, purchase firearms, file fraudulent tax returns, obtain government benefits, open bank accounts, connect telephone services, undergo surgery, file for bankruptcy, and even bear children.[33]

¶16 Victims are left to suffer in unique ways, feeling angry, aggravated, and helpless all in the same breath. Those who have lived through identity theft will usually describe how their

---

[24] *See* Press Release, The Foundation For Taxpayer & Consumer Rights, Group Protests Citigroup's Anti-Privacy Lobbying By Skywriting CEO's Social Security Number, (Oct. 24, 2003), *available at* http://www.consumerwatchdog.org/corporate/pr/pr003764.php3 (last visited Mar. 21, 2004).

[25] Jeordan Legon, *'Phishing' scams reel in your identity*, *Feds pursue culprits, warn consumers*, CNN.COM, July 22, 2003, *at* http://www.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html (last visited Mar. 21, 2004).

[26] *Id.*

[27] *See Monster.com Warns About ID Theft*, WIRED NEWS, Feb. 27, 2003, *at* http://www.wired.com/news/business/0,1367,57852,00.html (last visited Mar. 21, 2004).

[28] *See* Sovern, *supra* note 23, at 345.

[29] *Id.*

[30] Stephen Mihm, *Dumpster-Diving for Your Identity*, N.Y. TIMES MAG., Dec. 21, 2003, at 45. (reporting that approximately one in a thousand acts of identity theft end with conviction of the offender, making "[i]dentity theft . . . a very lucrative, low-risk crime.").

[31] *See* FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT (2003), at 4, *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited Mar. 21, 2004); *see also* FED. TRADE COMM'N, NATIONAL AND STATE TRENDS IN IDENTITY THEFT (2003) *at* http://www.consumer.gov/idtheft/reports/CY2002ReportFinal.pdf (last visited Mar. 21, 2004).

[32] *See* Sovern, *supra* note 23, at 345.

[33] *See id.* at 349-50.

lives were catapulted into disarray, slowly ruined by a predator's destructive behavior, leaving nothing but an uncertain future.

A. SSN Not For Identification Purposes

¶17 So far, U.S. policymakers have tried to curb identity theft scams by creating tough criminal penalties for violators. Not only has criminalization failed to stop identity theft, but identity theft continues to flourish with no end in sight. At the heart of the crisis lies a pervasive pattern of chronic overdependence on using the SSN as *the* primary method of identifying individuals. Naturally, our society's heavy, widespread reliance on a nine-digit identifier creates an easy and appealing target for wily identity predators. This, however, was not always the case.

¶18 Originally, the SSN was created solely for the purpose of tracking workers' Social Security earnings records, not to identify people. At first, Social Security cards specifically said "Not For Identification Purposes."[34] Today, over 390 million SSNs have been generated,[35] but the cards no longer offer any disclaimer.

¶19 The situation slowly worsened over the years. Federal, state, and local governments soon recognized the universal value of the SSN. Federal and state legislatures enacted laws requiring SSN uses for a wide range of purposes unrelated to the Social Security program. For example, federal law requires SSNs be used to administer the federal personal income tax and Medicaid, Food Stamp, and Child Support Enforcement programs.[36]

¶20 Private industry quickly followed. With the credit card boom of the 1970s and 1980s, the industry gained SSN access to everyone with a credit history. By the early 1990s, the credit bureaus began selling their databases, full of valuable SSN and other identifying goodies, to just about anyone willing to buy it.[37] Through resellers, credit bureaus sold their information to credit providers, debt collectors, private detectives, lawyers, and even the so-called "business community."

B. Nine-Digit Key to Identity Theft

¶21 At this point, there is little hope of protecting SSN information, given the broad access group developed over the years. By allowing the SSN to be used beyond its original purpose, we have now lost control over its use. To some, the SSN is a financial time bomb—a powerful nine-digit key that unlocks the door to identity theft.[38] Universal in financial transactions, pervasive in universities as a student identification number, and overused for everyday recordkeeping, the SSN today is a valuable asset that is too often subject to abuse. [39]

---

[34] *See* Francis J. Menton, Jr., *Outside Counsel: Can You Protect Yourself From Identity Theft?*, N.Y. L.J., April 29, 2002, at 1.

[35] *Social Security Numbers: SSNs Are Widely Used by Government and Could Be Better Protected: Testimony Before the Subcomm.on Social Security*, *House Comm. on Ways and Means*, 107th Cong. 3 (2002) (statement of Barbara D. Bovbjerg, Director, Education, Workforce and Income Security Issues), *available at* http://www.consumer.gov/idtheft/reports/gao-d02691t.pdf (last visited Mar. 21, 2004).

[36] *See, e.g.*, 42 U.S.C. 405(c)(2)(C)(i) ("It is the policy of the United States that any State (or political subdivision thereof) may, in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction, utilize the social security account numbers issued by the Commissioner of Social Security for the purpose of establishing the identification of individuals affected by such law, and may require any individual who is or appears to be so affected to furnish to such State (or political subdivision thereof) or any agency thereof having administrative responsibility for the law involved, the social security account number (or numbers, if he has more than one such number) issued to him by the Commissioner of Social Security.").

[37] *See* Menton, Jr., *supra* note 34.

[38] Margaret Mannix, *Stolen Names, Stolen Lives*, U.S. NEWS & WORLD REP., Nov. 12, 2001, at 40, 41.

[39] *See* Mihm, *supra* note 30, at 46 (noting that even if every business in the country never threw away a single scrap of paper, identity predators would still be able to steal SSNs using inside contacts: "Some gangs of identity thieves have relied on cleaning crews and temps with easy access to sensitive information.").

¶22 Our society's inexplicable overdependence on the SSN has come at a price. For identity theft victim Robert Horowitz, for example, the shocking part came when he learned that the individual who stole his identity repeatedly misspelled his name, and that his address, date of birth, and telephone number were all incorrect.[40] In fact, after obtaining copies of his credit report, Mr. Horowitz realized that the *only* piece of information that was accurate was his SSN. "So much credit was handed out based solely on my social security number and not on any kind of cross-references."[41] That explains why most identity predators simply rely on a name and a SSN to open credit card accounts, illegally enter or work in the United States, or conceal their true identity as part of a larger criminal plot.

¶23 However, given its unfettered power—and our gross overdependence on its unique identifying features—the SSN poses a risk to even the most wary consumers. For example, shortly after Pennsylvania enacted its identity theft protection statute, one of the authors of the law, Representative Matthew Baker, discovered that someone had stolen his identity.[42]

¶24 Describing the grim state of affairs to a congressional subcommittee, New York City Police Detective Michael Fabozzi, an expert in identity theft crimes, pointed out that the present system is not just vulnerable, but also leaves victims to fend for themselves trying to clear their credit histories and good names.[43] Even after victims demonstrate that fraud occurred, lenders and credit reporting agencies are often uncooperative in taking steps to prevent further damage from occurring, and persist in assigning the imposter's transactions to the victim. Thus, existing figures fail to quantify the burden of proof identity theft victims must bear, or the time investment victims must make, just to reclaim their stolen identities.

¶25 In January 2003, federal agents charged Philip Cummings and several others with conspiracy to commit fraud as part of the largest identity theft case in U.S. history.[44] Quite the opposite from the mythical hacker stealing identities from a gloomy basement, Mr. Cummings worked as a customer service representative at a software company that allowed banks and other lending institutions to get commercial credit information from the three largest U.S. credit agencies: Equifax, TransUnion, and Experian.[45] Using his help-desk position to get access codes, Mr. Cummings sold vital personal information to criminals—affecting more than 30,000 victims, and costing $2.7 million in fraudulent charges.[46]

¶26 For some reason, most consumers think that others will use their SSNs responsibly, and protect them from unnecessary exposure. Unfortunately, the numbers suggest otherwise. An FTC Identity Theft Report published in September 2003 found that consumers in 2002 lost more than $5 billion from identity theft.[47] In 2002, identity predators stole nearly $50 billion from businesses and financial institutions, or an average of $10,200 per victim.[48] Average out-of-pocket expenses for victims to remedy their credit problems was roughly $1,200 per person.[49] On top of the financial burdens, investigators estimate that victims spent an average of sixty hours, or 300 million hours collectively, to repair the damage

---

[40] *Protecting Privacy and Preventing Misuse of the Social Security Number, 2000: Hearings on H.R. 4857 Before the Subcomm. on Soc. Sec. of the House Comm. on Ways and Means*, 106th Cong. (2000) (statement of Robert Horowitz, Business Owner, Boca Raton, Florida).

[41] *Id.*

[42] *See* Mannix, *supra* note 38, at 41.

[43] *Protecting Privacy and Preventing Misuse of Soc. Sec. Numbers, Before the Subcomm. on Soc. Sec. of the House Comm. on Ways and Means H.R.*, 107th Cong. (2001) (statement of Michael Fabozzi, Detective, Computer Investigations and Technology Unit, New York City Police Department, New York).

[44] *See* Renay San Miguel, *Tackling Identity Theft*, CNN HEADLINE NEWS, January 29, 2003, *available at* http://edition.cnn.com/2002/TECH/11/26/hln.wired.id.theft (last visited Mar. 21, 2004).

[45] *Id.*

[46] *Id.*

[47] *See* FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT, supra note 31, at 6-7.

[48] *Id.*

[49] *Id.* at 6-7, 43.

inflicted by identity predators.[50] Many victims report missing several days or weeks of work to deal with creditors, employers, and law enforcement officials. Some victims even lose their jobs, their homes, and must file for bankruptcy protection.

¶27 Sensitive to market demands, insurance companies began offering nervous policyholders identity theft policies to help recover administrative costs.[51] In general, identity theft insurance policies reimburse victims for lost wages, transaction costs, and legal expenses of up to $25,000.[52]

¶28 Even so, statistics often fail to accurately track the number of incidents, because many victims do not discover they have been victimized until months (or sometimes years) later when they apply for a loan or creditors try to collect unpaid debts. The 2003 FTC Identity Theft Report found that most identity fraud victims never notify the police, and only 37% notify a credit bureau.[53]

C. Criminal Identity Theft

¶29 Emerging as a serious public safety concern is "criminal identity theft." According to the FTC, 4% of all identity theft victims reported that their personal information was misused to evade legal sanctions or criminal penalties.[54] In criminal identity theft, a perpetrator eludes prosecution by using a victim's stolen identity on arrest, say for a traffic violation, shoplifting, marijuana possession, or other misdemeanor charge. When the perpetrator fails to appear in court, a warrant is issued to arrest the identity theft victim, not the actual offender. The warrant may go unused for quite some time, until finally the victim is stopped for a traffic violation, undergoes a background investigation in connection with a new job, or passes through customs after returning from a foreign visit.

¶30 To understand in human terms the devastating effect of criminal identity theft, we turn to Dawn and Margaret. Dawn awoke late one night to answer the phone. On the line was a man claiming to be her attorney who rambled on about her failure to appear in court the day before, a forfeited $10,000 bond, and a warrant for her arrest.[55] Shocked by the call—and the fact that she had never actually been arrested—Dawn agreed to meet with prosecutors the next day.[56] At this meeting, Dawn learned she had fallen victim to criminal identity theft. Using Dawn's name and address, an imposter was charged in federal court with passing a forged Treasury check, and possession of stolen mail.

¶31 For Margaret, the frustration lasted several months while she tried in vain to get her financial institution, Nations Bank, to close a fraudulent checking account opened in her name after her wallet was stolen. Never expecting that her bank's transactional blunder could land her in jail, Margaret was eventually arrested at her home, in front of her son, on thirteen warrants stemming from charges of issuing bad checks.[57] To Margaret, the experience was both hurtful and embarrassing.[58]

¶32 In most cases, criminal identity theft victims are arrested until such time that they successfully prove that an identity predator is to blame. This usually means that most criminal identity theft victims are victimized twice: once by thief, the again by the system.

---

[50] *Id.* at 6-7, 45.
[51] *See* Sharon Epperson, *Insurance Coverage for ID Theft*, MSNBC NEWS, May 8, 2003, *at* http://www.msnbc.com/news/910153.asp?0cv=TB10 (last visited Mar. 21, 2004).
[52] *See Stop Thieves from Stealing You*, CONSUMER REP., Oct. 2003, at 14 (concluding that given the limited coverage, identity theft insurance not worth the money).
[53] *See* FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT, *supra* note 31, at 9.
[54] *Id.* at 6.
[55] *See* Stephen F. Miller, *Someone Out There Is Using Your Name: A Basic Primer on Federal Identity Theft Law*, 50 FED. LAW. 11 (2003).
[56] *Id.*
[57] *Falsely Arrested*, CONSUMER REP., Oct. 2003, at 13.
[58] *Id.*

Fortunately, in Dawn's case, she was exonerated after the phony Dawn was arrested by federal authorities one month later for trying to cash yet another check using the name of another victim.[59] For Margaret, it took five court appearances in two counties to clear her good name. She eventually won a $300,000 negligence verdict against Nations Bank for its failure to verify key information before opening the account.

D. Federal Law Prohibiting Identity Theft

¶33 Until recently, identity theft was only handled at the local level. But in 1998, Congress enacted the Identity Theft and Assumption Deterrence Act ("ITADA"),[60] effectively making identity theft a federal crime. Specifically, the statute prohibits individuals from knowingly transferring or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.[61]

¶34 Congress also instituted new penalties for identity predators. A violation can be punishable by up to fifteen years in federal prison if the identity thief obtains anything worth more than $1,000 in total or more during any one-year period.[62] If the amount of loss is under $1,000, the offense carries a maximum sentence of three years.[63]

¶35 Under 18 U.S.C. § 1028(a)(7), "means of identification" does not require the production, possession, or use of an actual identification document. Instead, "means of identification" is broadly defined to include a wide range of personal identifying information. The definition includes any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any name, SSN, date of birth, official state or government-issued driver's license or identification number, alien registration number, government passport number, or employer or taxpayer identification number.[64]

¶36 Apart from ITADA, two other federal statutes require governmental entities to protect individual information. One is the Privacy Act,[65] which requires government agencies to protect the privacy rights of individuals whose records it may possess. This means federal agencies are prohibited, except in special prescribed circumstances, from disclosing an individual's SSN without his or her written consent. The other is the Gramm-Leach-Bliley Act,[66] which applies to the financial services industry, and protects "nonpublic personal information," like SSN information.

¶37 Still, no single federal law regulates how the SSN is used in the private sector. This would explain why so many businesses, organizations, and universities routinely use the SSN as a data management tool to run their day-to-day operations. In fact, private companies are free to deny anyone credit, service, or membership for refusing to furnish their SSN. Simultaneously, and contrary to popular belief, the Social Security Administration has no power to control how private entities use their account numbers. The result is an extremely vulnerable system that puts the entire burden on the consumer. With no power to control how their SSNs are kept, used, or distributed, consumers are left to simply sit and wait for an identity thief to strike.

---

[59] *See* Miller, *supra* note 55, at 11.
[60] 18 U.S.C. § 1028.
[61] 18 U.S.C. § 1028(a)(7).
[62] 18 U.S.C. § 1028(b)(1)(D).
[63] 18 U.S.C. § 1028(b)(2)(A)-(B).
[64] 18 U.S.C. § 1028(d)(4).
[65] 5 U.S.C. § 552a.
[66] 15 U.S.C. §§ 6801-6827

E. TRW Inc. v. Andrews

¶38 A good example of consumer vulnerability in the Information Age is set out in *TRW Inc. v. Andrews*—the first identity theft case decided by the U.S. Supreme Court. The 2001 case involved a patient who fell victim to identity theft after her doctor's former receptionist stole her SSN information from an intake form, and opened several credit accounts.[67] The plaintiff, Adelaide Andrews ("Andrews"), visited a radiologist's office in Santa Monica, California on June 17, 1993.[68] After completing a new patient form, and disclosing her name, date of birth, and SSN, Andrews handed the form to the office receptionist, Andrea Andrews ("Impostor"). The Impostor copied Andrews's SSN information, and illegally used it to solicit credit from four different companies.[69] All four companies requested a report from the credit reporting agency TRW (now Experian), but only one of them approved the Impostor's credit application.

¶39 On May 31, 1995, Andrews learned of the Impostor's fraudulent activities after she tried to refinance her home and, in the process, obtained a copy of her credit report.[70] On October 21, 1996, almost seventeen months after she discovered the Impostor's conduct, and more than two years after TRW's first two disclosures, Andrews filed suit in federal district court.[71] In her complaint, Andrews alleged that TRW negligently failed to verify Andrews's identity before disclosing her credit information.[72] Andrews asserted that TRW facilitated the Impostor's illegal activities by disclosing information based only on matching SSN information, last name, and first initial, but failing to verify other key identifiers like date of birth, address, and first name.[73]

¶40 However, the case did not focus on the consequences of lax credit agency disclosure policies. Instead, the Supreme Court agreed to hear the case to resolve one issue: whether the statute of limitations in actions against a credit reporting agency under the Fair Credit Reporting Act[74] ("FCRA") begins when the plaintiff discovers the violation (the injury discovery rule) or when the violation initially occurs (the violation occurrence rule).[75] In its 9-0 decision, the Supreme Court held that the two-year statute of limitations to bring an action under the FRCA begins when the alleged wrongful disclosure occurs (violation occurrence), not when an individual discovers the wrongful disclosure.[76] The Court rejected the Ninth Circuit's presumption that a discovery rule applies for all federal statutes of limitations unless Congress expressly legislates otherwise.[77] The Court concluded that Congressional intent to deny a general discovery rule does not need to be explicit, as the Ninth Circuit held, but can be implied from the text and structure of the statute.[78]

¶41 The practical effect of this decision is that it puts the burden on consumers to routinely check their credit reports or find themselves unable to sue credit reporting agencies with lax information sharing policies.

---

[67] TRW Inc. v. Andrews, 534 U.S. 19 (2001).
[68] *Id.* at 23.
[69] *Id.* at 24.
[70] *Id.*
[71] *Id.*
[72] *Id.* at 25.
[73] *Id.*
[74] *See generally* 15 U.S.C. § 1681
[75] TRW Inc. v. Andrews, 534 U.S. 19, 26 (2001); *See also* Erin M. Shoudt, *Identity Theft: Victims "Cry Out" for Reform*, 52 AM. U. L. REV. 339, 353 (2002).
[76] *Andrews*, 534 U.S. at 30.
[77] *Id.* at 28 ("The Ninth Circuit thus erred in holding that a generally applied discovery rule controls this case.").
[78] *Id.*

F. Congressional Attempts to Curb Identity Theft

¶42 Recently, federal legislators have proposed several bills intended to protect consumers from SSN misuse. Not surprisingly, the proposals vary in scope, trying to balance consumer protection concerns with corporate efficiency interests. Some bills would prohibit by private entities the sale, purchase, or display of SSN information. Others would penalize any entity that would deny goods or services to individuals who refuse to furnish their SSNs.

¶43 Sample legislative proposals include bills that would prohibit the sale, purchase, or display of SSNs by governmental agencies or private companies.[79] Several bills also prohibit any appearance of SSN information on driver's licenses or motor vehicle registrations.[80] Others proscribe governmental agencies from displaying SSNs on identification cards.[81]

¶44 To be effective, however, new SSN protection laws must prevent private companies from denying goods or services to anyone unwilling to furnish their SSN, and prohibit public and private entities—like public and private universities or student loan administrators—from using the SSN as their primary account number.

¶45 New legislation addressing identity theft should be simple, based on fair information practices, and include few exceptions or loopholes. At the same time, any new law should also build on—not weaken or overlap with—existing privacy protections, including those of the Privacy Act or the Gramm-Leach-Bliley Act. Above all, any new law should limit SSN use to only those purposes that benefit the number holders, not information brokers, mass marketers, or other entrepreneurs that carelessly expose it to abuse by making it available for a fee.

¶46 Proponents of greater protections for consumers, like Professor Jeff Sovern, also suggest holding credit reporting agencies liable for reporting the transactions of an imposter as those of a victim.[82] Right now, FCRA provisions hold creditors liable for misreporting information under one of two situations. The first is for furnishing information to a credit reporting agency knowing, or consciously avoiding knowing, that the information is inaccurate.[83] The other is when they have been notified by the consumer of the erroneous information and the information is in fact inaccurate.[84] Even when creditors violate these provisions, consumers still do not have a private claim against them.[85] The result, as described by Professor Sovern, is that creditors have little incentive to make sure that their reports to the credit bureaus are accurate.[86]

¶47 To ease the public's concern, federal lawmakers included a number of changes to the updated version of the FCRA aimed at reducing identity theft incidents, improving the resolution of consumer disputes with financial institutions, and modifying the use of and access to consumer credit information. The final product, known as the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), has some protections for consumers, but still leaves a number of gaps unsealed. For example, FACTA requires credit reporting agencies to provide free annual reports to consumers, block information resulting from identity theft, and offer "active duty alerts" on credit reports belonging to active military personnel.[87] Credit reporting agencies must also "reconvey" fraud alerts placed by consumers to those

---

[79] Social Security Number Privacy and Identity Theft Act, S. 1014, H.R. 2036, 107th Cong. (2001).
[80] *Id. See also* Privacy Act of 2003, S.745, 108th Cong. (2003).
[81] *See* Social Security Number Misuse Prevention Act, S.848., 107th Cong. (2001); Personal Information Privacy Act, H.R. 1478, 107th Cong. (2001).
[82] *See* Sovern, *supra* note 23, at 406.
[83] 15 U.S.C. § 1681s-2(a)(1)(A).
[84] 15 U.S.C. § 1681s-2(a)(1)(B).
[85] 15 U.S.C. § 1681s-2(c).
[86] *See* Sovern, *supra* note 23, at 406.
[87] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, H.R. 2622, §§ 202, 205, and 501, 108th Cong. (2003). *See also*, S. 1753, §§ 112, 152, and 211.

entities seeking a consumer's credit report,[88] and take steps to reconcile address discrepancies, if the address on record "substantially differs" from the one submitted by the credit report requester.[89] Unfortunately, the statute does not define the term "substantially differs," so this well-meaning provision may, in practice, amount to little if broadly interpreted.

¶48 The FACTA also imposes new requirements on members of the financial services industry and other entities that furnish consumer credit information. Among them, the new statute prohibits the "repollution" of consumer reports. This means that a furnisher of consumer credit information cannot submit information to a credit reporting agency if a consumer has provided the furnisher with a police report showing that the charges were caused by identity thieves.[90] However, the statute is silent about the consequences to creditors who fail to comply with this provision. Financial institutions will also be required to truncate credit and debit card account numbers in all electronic transactions. This provision will prohibit merchants from printing the expiration date or more than the last 5 digits of the consumer's card number at the point of sale or transaction.[91]

¶49 Finally, limitations on affiliate sharing are also part of the law's effort at reform. Specifically, consumers must be afforded the "opportunity to prohibit all solicitations for marketing purposes, and may allow the consumer to choose from different options when electing to prohibit the sending of solicitations, including options regarding the types of entities and information covered, and which methods of delivering solicitations the consumer elects to prohibit."[92] Still, this section will not apply to entities that have a pre-existing relationship with a consumer or their corporate affiliates.

G. Increased Protection: The Key to Improvement

¶50 In setting out to restore identity protection to the American public, Congress must enact prophylactic legislation. Given the alarming trends in identity theft schemes through SSN misuse, legislators must come up with viable options that will address the situation. Although the Internet clearly improves our daily lives by personalizing services and providing access to vast amounts of information at the click of a mouse, the high-tech social and economic prospects for the future will never materialize in the United States, so long as a person's entire identity remains uniquely vulnerable to theft by the simple compromise of a nine-digit government-issued account number. Therefore, encouraging public and private entities to overcome their SSN dependency would be a good place to start.[93]

¶51 Until recently, identity fraud victims were expected to undertake the time-consuming task of contacting every credit bureau, and bear the burden of proving that they are not in fact "dead beats." In 2003, however, the FTC introduced a uniform affidavit for victims to alert companies when identity theft occurs.[94] Many state and federal agencies publish comprehensive contact information, toll-free telephone numbers, and general suggestions on their websites to help consumers protect themselves against identity theft.[95] Among them, the agencies warn that before revealing any personally identifiable information, consumers

[88] H.R. 2622, § 202(i)(7). S. 1753, § 112(f) and (g).
[89] H.R. 2622, § 401. S. 1753, § 316.
[90] H.R. 2622, § 402. S. 1753, § 154.
[91] H.R. 2622, § 203. S. 1753, § 113.
[92] S. 1753, § 214.
[93] *See, e.g.*, Menton v. Experian Co., 2003 WL 941338 (S.D.N.Y. Mar. 6, 2003) (finding unpersuasive Experian's argument that "proper identification" as defined by the FCRA should be narrowly construed to mean that, in all circumstances, a consumer must provide his Social Security number in order to receive his credit report).
[94] Press Release, Fed. Trade Comm'n, Federal Trade Commission Announces ID Theft Affidavit, *at* http://www.ftc.gov/opa/2002/02/idtheft.htm (last visited Mar. 21, 2004).
[95] *See, e.g.*, the Social Security Administration's website, *at* http://www.ssa.gov; the Federal Trade Commission's website, *at* http://www.ftc.gov and http://www.consumer.gov; and the Florida Attorney General's Office, *at* http://myfloridalegal.com/consumer.

should ask how that information will be used and whether it will be shared with others. Also, consumers should pay attention to billing cycles, guard their mail from theft, and provide their SSN only when absolutely necessary. For a fee, private companies are even offering identity protection monitoring services online that warn consumers when signs of fraud appear on their credit reports.

¶52 Still, in a system where consumers do not have a choice about how their information is collected, shared, or used, the fallacy underlying these measures is that they presume consumers actually can control the personal information already given to banks, credit card companies, landlords, employers, and online services. But the opposite is true. With little control over their own personal information, savvy consumers should proceed with extreme caution before sharing any sensitive information about themselves with anyone. [96]

¶53 In sum, information accuracy and identity theft prevention are vital elements to improving our current state of affairs. To quote Treasury Secretary John Snow, "Secure, reliable information is the lifeblood of all financial services, among which consumer credit is fundamental. It is not an overstatement to suggest that preserving the integrity and availability of consumer credit in this economy is preserving prosperity itself."[97]

II. CYBERSTALKING: A VIRTUAL FEAR FACTOR FOR VICTIMS

¶54 Next, we shift our focus to another up-and-coming offense uniquely facilitated by the Internet's immense global network: cyberstalking. Although no universal definition exists, cyberstalking occurs when an individual or group uses the Internet, e-mail, or other electronic communications to stalk or harass another.[98] Much like offline stalking, cyberstalking involves harassing or threatening behavior repeatedly performed using e-mail, chat rooms, bulletin boards, or instant messages.[99] These actions may or may not be accompanied by a credible threat of serious harm, and they may or may not be precursors to an assault or murder.[100] Unlike offline stalking, however, a cyberstalker does not need to be physically near the victim.

¶55 This uncertainty can cause a greater sense of panic among victims who are left to wonder if the cyberstalker is in another state, down the block, or in the next cubicle at work.[101] Victims seldom know if the cyberstalker is a former lover, a total stranger met in a chat room, or simply a random prank from a twisted mind.

¶56 In one electronic cry for help, a distressed cyberstalking victim wrote:

> *A friend of mine and I have both received threats from a certain individual but we are uncertain how much information is needed to prosecute and how credible that information has to be. She has obtained a lawyer but he does not work in*

---

[96] *See* Mihm, *supra* note 30, at 46 (recognizing that while the actual identity thieves are to blame for any harm to the victims, the companies safeguarding sensitive records should share responsibility. "There is no 'standard of care' to which these companies are held. . . . If someone in [an] organization steals credit reports, the company is not responsible. The bottom line is that the banks and financial institutions are not held liable. [A]ll you need is some idiot, some young kid working at a hospital or bank who's not happy with his job, who's not making enough money. He'll sell you Social Security numbers.").

[97] Press Release, U.S. Secretary of the Treasury John Snow, Remarks Advocating the Renewal of the Fair Credit Reporting Act, June 30, 2003, *available at* http://www.ustreas.gov/press/releases/js515.htm (last visited Mar. 21, 2004).

[98] See Harry A. Valetk, *Cyberstalking: Navigating a Maze of Laws*, N.Y. L.J., July 23, 2002.

[99] *See generally* PATRICIA TJADEN & NANCY THOENNES, STALKING IN AMERICA: FINDINGS FROM THE NATIONAL VIOLENCE AGAINST WOMEN SURVEY, National Institute of Justice Centers for Disease Control and Prevention 1 (1998) ("Stalking generally refers to harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. These actions may or may not be accompanied by a credible threat of serious harm, and they may or may not be precursors to an assault or murder.")

[100] *Id.*

[101] VIOLENCE AGAINST WOMEN OFFICE, U.S. DEP'T OF JUSTICE, STALKING AND DOMESTIC VIOLENCE: REPORT TO CONGRESS 3 (2001).

> *cyber law. We fear our lives and our possessions. We know who the stalker is, the computers he is using to threaten us and where he lives. The man used to be a friend. What kind of protection do we have? And what can we do to get that protection?*[102]

¶57 For many victims, cyberstalking means enduring terror for months before seeking help. Even after a victim decides to ask for help, few know where to turn. Many local police departments still lack proper training and resources to investigate cyberstalking cases. As a result, a police officer might suggest that a victim contact their Internet Service Provider ("ISP") for technical assistance or "shut off" their computers.

¶58 But shutting off a computer is seldom enough. The common misperception is that since cyberstalking does not involve physical contact, it is less dangerous than offline stalking. The opposite is true. As more of us make the Internet an integral part of our personal and professional lives, stalkers can terrorize victims with personalized threats, hijack their computer using Trojan horse programs,[103] or access the wealth of personal information available online.

A. Non-confrontational, Impersonal, and Anonymous

¶59 Unlike their offline counterparts, cyberstalkers also enjoy a considerable advantage using the Internet's non-confrontational, impersonal, and anonymous features. In a 1999 report, the U.S. Department of Justice warned Internet users about a cyberstalker's allure to the Internet:

> [W]hereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. . . . As with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence.[104]

¶60 Unfortunately, cyberstalking is on the rise.[105] A 2003 poll conducted by an Internet job site found that one in six office workers in the United Kingdom had been harassed by e-mail.[106] According to the study, individuals in higher office positions were more likely to fall victim to e-mail harassment than their support staff.[107] While only 15% of secretaries claimed to be the victims of verbal attacks by e-mail, 28% of their bosses were harassed via their inboxes.[108] A 2003 study by WiredSafety.org[109] also found that women aged eighteen

---

[102] E-mail sent to LegalEagles at WiredPatrol.org (May 10, 2002) (copy on file with author).

[103] A Trojan horse program is a program that neither replicates nor copies itself, but causes damage or compromises the security of another computer. Typically, Trojan horse programs are spread by e-mail, arriving in the form of a joke program or other seemingly innocuous software. Technically, Trojan horse programs are not viruses since they do not replicate, but they can still be just as destructive. *See* Symantec Glossary of Terms, "Types of Threat: Trojan Horse," *at* http://securityresponse.symantec.com/avcenter/refa.html#t (last visited Mar. 21, 2004).

[104] U.S. DEP'T OF JUSTICE, 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (report from the Attorney General to the Vice President), *available at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (last visited Mar. 21, 2004).

[105] *See* DOJ, STALKING AND DOMESTIC VIOLENCE, *supra* note 101, at 3.

[106] *Email bullying on the rise*, BBC NEWS, Mar. 31, 2003, *at* http://news.bbc.co.uk/2/hi/technology/2902777.stm (last visited Mar. 21, 2004).

[107] *Id.*

[108] *Id.*

[109] WiredSafety.org, a 501(c)(3) non-profit corporation run entirely by volunteers worldwide, is an Internet safety, help, and education organization. More information is available at http://www.wiredsafety.org.

to thirty-two are at the greatest risk of cyberstalking.[110] While women remain the most likely targets, female cyberstalkers increased from 25% of all cyberstalkers in 2001 to 40% in 2002.[111]

¶61 In addition, a growing number of children are cyberstalking other children. School officials are also finding that bullying online is the latest, most vicious trend in children's social cruelty.[112] With the click of a button, tech-savvy kids are e-mailing rumors, posting defamatory statements, and inflicting permanent social damage on rival clique members. Published reports estimate that 16% of eleven- to nineteen-year-olds have received threatening text messages on their mobile phones.[113]

¶62 Based on these trends, we see that the Internet can play a unique role in creating a threat to personal safety, particularly when cyberstalkers use it to incite others against their victims. With minimal effort, cyberstalkers can impersonate their victim, simultaneously send lewd e-mails to employers, post inflammatory messages on multiple bulletin boards, and offend hundreds of chat room participants. The victim is then banned from bulletin boards, accused of improper conduct, and flooded with threatening messages from incensed cyber-community members. Thus, by taking advantage of the Internet's anonymous nature, a cyberstalker can wreak havoc on a victim without ever making any direct contact. Law enforcement officials are then faced with great technological obstacles to identifying, locating, and arresting the offender.[114]

¶63 For all these reasons, the danger from cyberstalking is real, and the consequences of neglect are tragic. In 2001, for example, a Massachusetts man was sentenced to five years in prison after he pleaded guilty to stalking and raping a fourteen-year-old girl he met in a chat room.[115] In another case, a man harassed a nine-year-old girl for more than two years by sending her postings soliciting sex. Surviving this traumatizing ordeal, the girl's mother confessed that "[I]t never occurred to me that the Internet could be used as a weapon."[116]

¶64 In 1999, a University of San Diego graduate student was arrested after he terrorized five female university students for more than one year by bombarding them with hundreds of violent and threatening e-mails.[117] The victims endured up to four or five e-mails a day containing violent threats like "Reply to My Email or You Will Die."[118] Another e-mail stated, "I'll give you until this Friday to answer my e-mail or I'll show up at your cell physiology class or go to your house."[119] The graduate student-turned-cyberstalker pled guilty, and told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him.[120]

---

[110] WIREDSAFETY.ORG, WIREDSAFETY 2003 CYBERSTALKING STUDY, *at* http://www.wiredpatrol.org/documents/cyberstalking_study.ppt (last visited Mar. 21, 2004).

[111] *Id.*

[112] Rachel Simmons, *Cliques, Clicks, Bullies And Blogs*, WASH. POST, Sept. 28, 2003, at B1 (reporting that minors are resorting to interactive technologies to humiliate and bully their peers).

[113] Jo Twist, *Text blocking aid fights bullies*, BBC NEWS, Oct. 1, 2003, *at* http://news.bbc.co.uk/1/hi/technology/3152628.stm (last visited Mar. 21, 2004).

[114] DOJ, 1999 REPORT ON CYBERSTALKING, *supra* note 104.

[115] *See Lowell man pleads guilty to Internet stalking, raping 14-year-old girl*, ASSOC. PRESS, Aug. 21, 2001, *available at* http://www.boston.com/news/daily/21/internet_stalker.htm (last visited Mar. 21, 2004).

[116] Rebecca Raphael, *Stalking in Cyberspace, New Medium, Old Crime*, ABCNEWS.COM, Feb. 24, 2002, *at* http://abcnews.go.com/onair/2020/2020_000224_cyberstalker_feature.html (copy on file with author).

[117] *See* DOJ, 1999 REPORT ON CYBERSTALKING, *supra* note 104, at 5.

[118] *See* Joseph C. Mershman, *The Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation*, 24 HARV. WOMEN'S L.J. 255 (2001) (citing Suzanne Choney, *Stalking in Cyberspace: Cases Start to Grow, Along With Computer Use*, SAN DIEGO UNION-TRIB., June 22, 1999, at 6).

[119] *Id.*

[120] *Id.*

B. Different Laws For Different Folks

¶65 Overlooking the fact that cyberstalking is a multi-jurisdictional crime, federal legislators have yet to enact adequate statutory protections for cyberstalking victims. Instead, existing anti-stalking statutes at the federal level are ill-suited to confront the evils of cyberstalking because of their focus on physical contact.

¶66 For example, under 18 U.S.C. § 875(c), individuals who transmit any threat to kidnap or injure another person face up to five years in prison and fines of up to $250,000.[121] But this statute has several limitations. First, 18 U.S.C. § 875(c) only applies to communications of actual threats and cannot be used in a case where a stalker engaged in a pattern of conduct intended to harass or annoy another.[122] Second, 18 U.S.C. § 875(c) may not apply to situations where a cyberstalker harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy a victim.[123]

¶67 Another statute, 47 U.S.C. § 223, prohibits the use of a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the number called.[124] This statute requires that the perpetrator withhold his or her name.[125] Still, the statute does little to combat the evils of cyberstalking head-on. While 47 U.S.C. § 223 is broader than 18 U.S.C. § 875, covering both threats and harassment, § 223 applies only to direct communications between stalker and victim. Therefore, like § 875, § 223 also fails to address situations where a cyberstalker harasses or terrorizes another by posting messages on a bulletin board or in a chat room inciting others to harass or annoy a potential victim.

¶68 A third statute, the Interstate Stalking Punishment and Prevention Act of 1996, prohibits any person from traveling across state lines with the intent to injure or harass another person and, in the course of such action, placing that person or a member of their family in a reasonable fear of death or serious bodily injury.[126] However, this statute's emphasis on physical travel and personal contact is wholly inadequate to thwart a cyberstalker's virtual terror tactics.

¶69 Finally, federal law protects children from certain hostile online activities. Specifically, under 18 U.S.C. § 2425, it is a crime to use any means of interstate or foreign commerce (like a telephone or the Internet) to communicate with any person with intent to solicit or entice a child under age sixteen into unlawful sexual activity.[127] Like its three legislative counterparts, this statute fails to explicitly prohibit harassing messages or other cyber-terror tactics directed to minors, absent a showing of intent to entice or solicit the child for illicit sexual purposes. Combined, federal statutes currently in place that proscribe offline stalking fail to adequately protect Internet users from stalking in cyberspace.

C. A Smorgasbord of State Laws

¶70 In the absence of a clearly defined federal cyberstalking crime, state legislatures have drafted their own detailed anti-cyberstalking laws. Unfortunately, the result is a complicated maze of state laws that creates confusion with varying definitions, protections, and penalties.

---

[121] 18 U.S.C. § 875(c) (2000); 18 U.S.C. § 3571(b)(3) (2000) (setting a maximum fine of $250,000 for a felony conviction).

[122] *See* 18 U.S.C. § 875 (2000).

[123] *See* DOJ, STALKING AND DOMESTIC VIOLENCE, *supra* note 101, at 10.

[124] 47 U.S.C. § 223 (2000). *See also* Am. Civil Liberties Union v. Reno, 929 F.Supp. 824, 829 n.5 (E.D. Penn. 1996), *aff'd*, 521 U.S. 844 (1997) (finding the term "telecommunications device" under 47 U.S.C. § 223 does not insulate individual user from liability for criminal behavior), *aff'd*, 521 U.S. 844 (1997).

[125] 47 U.S.C. § 223(a)(1)(C) (2000).

[126] *See* 18 U.S.C. § 2261A (2000).

[127] 18 U.S.C. § 2425 (2000). *But see* Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (striking portions of the Child Pornography Prevention Act outlawing virtual child pornography as unconstitutionally vague. Specifically, the Court struck two provisions: 18 U.S.C. §§ 2256(8)(B) and (D), which prohibited any depiction that "appeared to be" or "conveyed the impression" of child pornography).

¶71 As of March 2004, all but five states had laws expressly prohibiting harassing conduct through the Internet, e-mail, or other electronic means. In some states (like New York) cyberstalking is part of the general stalking or harassment laws; other states (like North Carolina) have a separate section under special computer crime legislation.[128] The general stalking or harassment laws of other states may be construed to cover cyberstalking without expressly stating that the Internet or e-mail is also covered.[129] Still, our current patchwork of local laws barely protects some victims, while altogether neglecting others.

¶72 To the detriment of victims, conflicting statutes at the state level—riddled with complex jurisdictional issues—deter law enforcement from ever getting involved. For example, Arizona's stalking statute only prohibits credible threats of violence against the victim, whereas California and South Carolina statutes prohibit threats against the victim's immediate family.[130] Maine residents enjoy substantial protection, since a stalker's course of conduct can constitute an implied threat.[131]

¶73 Penalties also vary. In New York, cyberstalking is a misdemeanor, while Illinois considers it a Class 4 felony.[132] In cases where cyberstalking is combined with offline stalking, heftier penalties usually apply.[133]

D. What's the Standard?

¶74 As mentioned above, differing statutory definitions and standards only serve to foster confusion. To be guilty of cyberstalking in Massachusetts, for example, the perpetrator must have intent to cause "imminent fear."[134] Conversely, in Minnesota and Texas, the perpetrator must only have knowledge (not necessarily intent) that he or she is causing fear.[135] To show fear, a victim's responses to the perpetrator's e-mails or other electronic communications can be important.

¶75 Most states require direct communication with the target (or family), but some states like Arkansas or Wisconsin require only sending a message that the person is likely to receive.[136] A common example of the latter would be an Internet message board or list messaging service. Most states also require that threats be against the person (or family) receiving the e-mail, while Washington goes so far as to prohibit threats against "any other person."[137] North Dakota's statute goes even further, defining harassment to include a threat to inflict injury on a person's reputation.[138] Other statutes include prohibitions against obscenity or lewd or profane language, but use of these are usually tied with intent to harass.[139] Another group of states include damage to property within the meaning of cyberstalking or cyber-harassment.[140]

¶76 Among the most generous definitions, Arizona's cyberstalking statute simply requires that a victim be "seriously alarmed" or "annoyed."[141] Illinois's statute also prohibits

---

[128] *Compare* N.Y. PENAL LAW § 240.30 (McKinney Supp. 2004), *with* N.C. GEN. STAT. § 14-196.3, ARK. CODE ANN. § 5-41-108(a)(1) (1997), *and* 720 ILL. COMP. STAT. § 5/12-7.5 (2002).
[129] *See, e.g.*, N.Y. PENAL LAW § 240.30.
[130] *Compare* ARIZ. REV. STAT § 13-2921 (2001), *with* CAL. PENAL CODE § 422 (1999), *and* S.C. CODE ANN. 16-3-1700(A)(2) (2003).
[131] *See, e.g.*, ME. REV. STAT. tit. 17A § 210-A (West Supp. 2003); COLO. REV. STAT. § 18-9-111 (Supp. 2003).
[132] *Compare* N.Y. PENAL LAW § 240.30 (making online harassment a Class A misdemeanor), *with* 720 ILL. COMP. STAT. § 5/12-7.5 (making cyberstalking a Class 4 felony).
[133] *See, e.g.*, N.Y. PENAL LAW § 215.51, VA. CODE ANN. § 18.2-60(A)(1) (1996).
[134] *See, e.g.*, MASS. GEN. LAWS ch. 265 § 43 (2002).
[135] *See, e.g.*, MINN. STAT. § 609.749 (2003), TX. PENAL CODE ANN. 42.07 (Vernon 2003).
[136] ARK. CODE ANN. § 5-41-108(a)(1) (1997); WIS. STAT ANN. § 947.0125 (West Supp. 2003).
[137] *See, e.g.*, WASH. REV. CODE ANN. § 9A.46.020,(1)(a)(i) (West Supp. 2004).
[138] N.D. CENT. CODE § 12.1-17-07 (Supp. 2003).
[139] *See, e.g.*, WIS. STAT ANN. § 947.0125 (West Supp. 2003).
[140] *See, e.g.*, HAW. REV. STAT ANN. § 711-1106(b) (Michie 1999).
[141] ARIZ. REV. STAT. § 13-2921 (2001).

spreading viruses.[142] Wisconsin's law is similar to that of Arkansas, but also prohibits anonymous e-mails or other actions that attempt to prevent disclosure of identity (if made with intent to harass).[143] Some statutes increase the offense from a misdemeanor to a felony if there were prior similar contacts with the victim, or prior similar bad acts.[144] A few states increase the penalty if the offender is a convicted felon.[145]

¶77 To complicate the matter, cyberstalking is not an occurrence that is solely domestic. A serious concern remains about cyberstalking attacks launched from foreign soil. A study published in New Zealand in June 2001 found that cyberstalking is a growing global concern of which the true prevalence remains unknown.[146] The problem, of course, is that even if other countries eventually enact laws prohibiting cyberstalking activities, applying international legal mechanisms to extradite and prosecute foreign offenders would be a daunting task.

E. RIAA v. Verizon

¶78 Despite the existing legislative mechanisms in place to protect Internet users from cyberstalking at the state level, courts interpreting copyright protection laws may on occasion inadvertently undermine user protections. In *Recording Industry Association of America v. Verizon*,[147] a federal district court in the District of Columbia created yet another vulnerability for Internet users when it held that an ISP must comply with a subpoena request for information under the Digital Millennium Copyright Act of 1998 ("DMCA").

¶79 The case began when the Recording Industry Association of America ("RIAA") served Verizon Internet Services ("Verizon") with a DMCA subpoena on July 24, 2002 to identify a Verizon subscriber believed to have made about 600 copyrighted songs available for downloading on a peer-to-peer network.[148] Verizon refused to comply with the RIAA's subpoena, arguing that since the alleged wrongdoing related to material transmitted over its network, and not actually stored on it, the RIAA's subpoena exceeded the scope of § 512(h) of the DMCA. Verizon read § 512(h) as applying only to those situations where the infringing material is physically stored on the ISP's network, whereas the RIAA argued that § 512(h) must be applied broadly to include information about the ISP's subscribers.

¶80 In defending its position, Verizon argued that a broad interpretation of § 512(h) could be used by cyberstalkers to issue fraudulent subpoenas, and obtain identifying information about potential victims like telephone numbers and addresses.[149] This legitimate safety concern stems from the simplicity of the § 512(h) expedited subpoena process. Under § 512(h), a copyright owner (or a person authorized to act on the owner's behalf) seeking an expedited subpoena must present to the clerk a proposed subpoena, a sworn declaration stating the information will be used only to legally protect copyrighted material, and a copy of the notification of claimed infringement.[150]

¶81 However, the district court rejected Verizon's arguments, concluding instead that the risk of cyberstalking was minimal.[151] The district court reasoned that the DMCA provided sufficient procedural mechanisms to detect fraudulent requests, and was hardly different from other statutes authorizing expedited subpoenas:

---

[142] *See* 720 ILL. COMP. STAT. § 135/1-2(a)(3) (2002).
[143] WIS. STAT ANN. § 947.0125(e)-(f).
[144] *See, e.g.*, GA. CODE ANN. § 16-5-90(d) (2003).
[145] *See, e.g.*, CAL. PENAL. CODE § 646.9(c) (West Supp. 2003).
[146] *See* ANGELA MAXWELL, CYBERSTALKING (2001), *available at* http://www.netsafe.org.nz/ie/downloads/cyberstalking.pdf (last visited Mar. 21, 2004).
[147] Recording Indus. Ass'n of Am. v. Verizon Internet Serv., 257 F.Supp.2d 244 (D. D.C. 2003).
[148] *Id.*
[149] *Id.* at 264-65
[150] *Id.* at 252 (citing 17 U.S.C. § 512(h)(1)-(2)).
[151] *Id.* at 265.

> Although conceivably one could falsify . . . information in a subpoena, the information is also easily verifiable by service providers, who can provide an additional check against fraudulent conduct. In fact, the remedial provisions of the DMCA, including the right to damages for misrepresentation, attorneys fees, contempt sanctions, and even the possibility of criminal perjury charges, should deter potential stalkers.[152]

¶82 On appeal, the U.S. Court of Appeals for the District of Columbia reversed the district court's decision, concluding instead that § 512(h) subpoenas may be issued only to an ISP engaged in storing infringing material on its servers.[153] ISPs acting as conduits for data transferred between two Internet users, such as persons exchanging e-mail or sharing P2P files, are not subject to § 512(h).

¶83 Although the appellate court's decision is a victory for privacy in cyberspace, at this point, it is still too early to predict how § 512(h) subpoenas, legislative initiatives, or current law enforcement mechanisms will affect cyberstalking in the United States or abroad. However, the issue deserves a closer look, since cyberstalking schemes have the potential to terrorize Internet users in ways not yet fully understood.

III. CYBERSPACE: A PERSONAL INFORMATION FLEA MARKET

¶84 Together, identity theft and cyberstalking share a common denominator: Both stem from informational privacy invasions. For either one to be carried out effectively, predators must first obtain some form of personal information about their prey. Enter the vast and ever-expanding world of cyberspace. As more of us become comfortable with using the Internet to conduct business and engage in everyday activities, we become more vulnerable to new types of privacy invasions. Indeed, with all the personal information available in cyberspace, the once obvious line between public and private realms becomes difficult to discern.

¶85 To tackle the problem, we must ask ourselves how much personal information we are willing to share with the rest of the world. Why has it become so easy for anyone to exploit personal information sources in cyberspace? What choices, if any, should consumers have to protect their personal information from unauthorized disclosures? Is personal informational privacy[154] an individual choice or a broader public policy concern?

A. No Explicit Right of Privacy

¶86 To begin with, the U.S. Constitution offers its citizens no explicit right of privacy. Instead, the U.S. Supreme Court has carved out zones of privacy based on several provisions in the Bill of Rights, for areas including marriage, procreation, contraception, family relationships, child rearing, and education.[155] In effect, the United States has chosen a sectored approach to privacy regulation so that records held by third parties, like consumer

---

[152] *Id.*

[153] Recording Indus. Ass'n of Am. v. Verizon Internet Serv, 351 F.3d 1229 (D.C. Cir. 2003).

[154] Information privacy (or data protection) refers to the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records.

[155] *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967) (finding Government's eavesdropping activities violated Fourth Amendment protections against unreasonable searches); Griswold v. Connecticut, 381 U.S. 479 (1965) (holding unconstitutional state statute prohibiting use of contraceptives); Paul v. Davis, 424 U.S. 714 (1976) (finding state may publicize a record of an official act such as an arrest).

marketing profiles or telephone calling records, are generally not protected unless a specific statute applies.[156]

¶87 Essentially, the American approach to privacy protection generally consists of self-regulation schemes, made up by industry coalitions, that implement policies to safeguard personal information.[157] Privacy legislation in the United States consists of a patchwork quilt of laws that are scattered among state and federal governments, offering limited protections in narrowly defined socioeconomic spheres (for example, health and financial privacy statutes). Under the recently-enacted Gramm-Leach-Bliley Act of 1999, for example, affiliated companies can share data with each other, and individuals must take affirmative action to prevent data sharing outside the affiliated group (known as "opting-out").[158]

B. Personal Information For a Fee

¶88 The mere thought that privacy might encompass an enforceable right to prevent the sharing of certain kinds of personally identifiable data arguably conflicts with our deeply held social values that elevate choice over constraint, freedom of speech over enforced silence, and sunlight over shadow.[159] This philosophy helps to explain why it has become so easy for anyone to exploit personal information sources in cyberspace.

¶89 In August 2003, the Foundation for Taxpayer and Consumer Rights ("Foundation") exposed the need for stronger information protection laws when it purchased confidential data belonging to several high-ranking U.S. officials.[160] Paying just $26 for each person, the Foundation obtained the SSNs and home addresses of CIA Director George Tenet, Attorney General John Ashcroft, and Presidential Chief Political Advisor Karl Rove.[161] In case the Foundation wanted to supplement its data with birth date information, it easily could have done so by visiting anybirthday.com. Anybirthday.com claims to have over 135 million birth dates readily available to anyone with Internet access—absolutely free. All you need is the first and last name of the individual whose birthday you wish to find. For a one-time $29 annual fee, anybirthday.com will also disclose anyone's home address. According to its privacy policy, the site's records are all derived from non-privileged public access information sources. "Information found in the Anybirthday.com database can be found elsewhere by anyone with a simple knowledge of public record access."[162]

¶90 Ironically, the vast majority of users in the United States have only a vague notion of just how much of their daily lives is systematically recorded in databases, and how little control they as consumers posses to control who collects and distributes their personal information.[163] Although much of the personal information collected about us is benign, increasing vulnerabilities in the way personal information is collected and maintained often lead to devastating consequences.[164] To some, the problem we face as consumers is not just

---

[156] *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

[157] Deborah M. McTigue, *Marginalizing Individual Privacy on the Internet*, 5 B.U. J. SCI. & TECH. L. 5, 44 (1999).

[158] 15 U.S.C. § 6802 (2000).

[159] Julie E. Cohen, *Cyberspace and Privacy: A New Legal Paradigm?*, 52 STAN. L. REV. 1373, 1375 (2000); *see also* Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 6-7 (1991) ("In general, scholarly analysis of the First Amendment disposes us toward the proposition that more information is better. We esteem sunlight because it illuminates.").

[160] *Group gets private data on Tenet, Ashcroft to underscore need for tougher laws*, U.S.A. TODAY.COM, Aug. 28, 2003, *available at* http://www.usatoday.com/tech/news/internetprivacy/2003-08-28-privacy-tenet_x.htm (last visited Mar. 21, 2004).

[161] *Id.*

[162] Anybirthday.com, Privacy Policy, *at* http://anybirthday.com/privacy.htm (last visited Mar. 21, 2004).

[163] *Id.*

[164] *Id.*

that vast amounts of personal information rest idly in countless, unknown databases, but that we as consumers have virtually no control over how that information is obtained, used, shared, or manipulated. As a result, we are left at the mercy of those who hold our data, and must trust them to guard it and use it in ways that will help and not hurt us.[165]

¶91 Once personal information reaches the liquid realm of cyberspace, the opportunities to exploit it are endless. Thanks to developments in information technology, website operators not only can gather individual data, but can also link it to one particular individual using neural networks, thereby making the stored data more valuable. Until now, data collection technology was limited to online interaction or other digital transactions, but broader tracking concerns lie ahead.

¶92 New experimental wireless tracking technology could one day meticulously monitor everything from the clothing on your back to the currency in your pocket. Known as radio frequency identification ("RFID"), this new tracking technology uses millions of special sensors to automatically broadcast the movement of merchandise when scanned with a radio signal. Huge retailers, like Wal-Mart, have started testing RFID systems, and proponents hail the "smart shelf" technology as the next-generation barcode that will allow merchants to streamline inventory and cut down on theft.[166] Farmers and pet owners currently use RFID systems to identify livestock and track their dogs and cats.[167] Finnish authorities recently developed RFID chips for travel cards and the European Central Bank plans on inserting them in EURO banknotes.[168] Dry cleaners and airport luggage systems may soon implement RFID systems to benefit from its versatile, wireless tracking technology.[169] One company is even testing RFID systems for use as implantable identification for humans with global positioning system technology that would allow remote tracking.[170]

¶93 With good reason, privacy advocates worry that RFID tracking systems could present unique concerns. At the retail level, RFID systems could gather unprecedented amounts of information about individual purchasing habits, and link it to detailed customer information databases.[171] Without a disabling feature, critics fear RFID systems would expose consumers to needless risk by allowing tech-savvy burglars to inventory a victim's house from a distance.[172] In some instances, RFID systems could also pose a fatal threat, if stalkers manage to adapt the technology to monitor a victim's belongings, embedded with RFID microchips, and track their whereabouts.

¶94 With so much personal information readily available in the public domain, information and communications technologies have managed to blur the once obvious line between public and private realms.[173] The difficult question confronting policymakers around the world today is how this new blurred reality can be reconciled with "the right to be let

---

[165] *Id.*

[166] Alorie Gilbert, *Privacy advocates call for RFID regulation*, CNET NEWS, Aug. 18, 2003, *at* http://news.com.com/2100-1020_3-5065388.html?tag=fd_top (last visited Mar. 21, 2004).

[167] David LaGesse, *They Know Where You Are*, U.S. NEWS & WORLD REP., Sept. 8, 2003, at 36-38.

[168] *See* CEDRIC LAURANT, PRIVACY & HUMAN RIGHTS 2003, AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS, *available at* http://www.privacyinternational.org/survey/phr2003/ (last visited Mar. 21, 2004).

[169] Matthew Broersma, *RFID chips sent to the dry cleaners,* ZDNET.COM, Aug. 12, 2003, *at* http://zdnet.com.com/2100-1103_2-5062542.html (last visited Mar. 21, 2004).

[170] *An ID Card That You Can Never Lose*, U.S. NEWS & WORLD REP., Sept. 8, 2003, at 38.

[171] Ephraim Schwartz, *RFID ripples through software industry*, INFOWORLD, Sept. 26, 2003, *at* http://www.infoworld.com/article/03/09/26/38NNrfid_1.html. (describing how vendors are rewriting their enterprise applications to integrate RFID data) (last visited Mar. 21, 2004).

[172] *See, e.g.*, Xeni Jardin, *Wireless Hunters on the Prowl*, WIRED NEWS, Jul. 2, 2003, *at* http://www.wired.com/news/wireless/0,1382,59460,00.html (last visited Mar. 21, 2004) (describing group of security experts and wireless enthusiasts in dozens of U.S. cities that roam around with Wi-Fi-sniffing gear, logging access points that will then be collected, shared, and analyzed).

[173] *See* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy As Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J., 1, 2 (1996) (noting use of computers to manage information has blurred delineation between public and private realms).

alone."[174] Can varying informational privacy policies coexist in an interconnected realm such as cyberspace? What legal duties, if any, do information brokers owe to third parties to make sure that the personal information they harvest and sell is managed responsibly?

C. Remsburg v. Docusearch, Inc.

¶95 No longer willing to ignore the consequences of privacy invasions and lax information-sharing policies, courts have begun to craft negligence standards. In *Remsburg v. Docusearch, Inc.*, the New Hampshire Supreme Court held that information brokers owe a duty to exercise reasonable care not to subject a third person to an unreasonable risk of harm.[175] In so holding, the court concluded that the family of a murdered young woman had grounds to sue the information broker hired by a stalker to locate his victim.

¶96 The *Remsburg* decision began with the tragic murder of Amy Lynn Boyer ("Amy"), a twenty-year-old woman from Nashua, New Hampshire. Amy was killed in 1999 when her stalker, Liam Youens ("Youens"), shot her in cold blood as she left work, and then turned the gun on himself.

¶97 The legal issue in the *Remsburg* arose from Youens's use of Docusearch.com, an Internet-based investigation and information service site operated by a private investigator in Florida, to find out everything he could about Amy. In five separate transactions with Docusearch, amounting to just $95 in fees, Youens was able to get everything he needed to track Amy's daily whereabouts. At first, Docusearch could not find Amy's work address, but after repeated requests from Youens, Docusearch hired a subcontractor, who deceived Amy into revealing her work address.[176] Eventually, Youens was able to obtain Amy's home address, date of birth, SSN, and the location of the dentist's office where she worked.

¶98 Recognizing the need to protect unsuspecting victims, the New Hampshire Supreme Court stated that "If a private investigator or information broker's disclosure of information to a client creates a foreseeable risk of criminal misconduct against the third person whose information was disclosed, the investigator owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm."[177]

¶99 In examining whether the threat of criminal misconduct is foreseeable, the Court specifically looked at two increasing risks associated with lax disclosure practices, stalking and identity theft:

> The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client. [T]his is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information.[178]

D. Clerk of the Court in Cyberspace

¶100 Few of us would be shocked to learn that federal, state, and local governments keep digitized records detailing individual addresses, income information, automobile ownership,

---

[174] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (declaring right "to be let alone" as a matter of personal privacy) (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (Callaghan & Co. ed., 2d ed.1888) (1878)).
[175] 816 A.2d 1001, 1006 (N.H. 2003).
[176] *Id.* at 1006.
[177] *Id.* at 1007.
[178] *Id.* at 1008.

car insurance, criminal records, marital status, real estate holdings, voter registration, and many other facets of our daily existence.[179] But news that this information is readily available online for free, or to anyone willing to pay a nominal fee, would likely evoke a much different reaction.

¶101 Consider the popular movement to digitize legal records historically found only in dusty cellars, and make them available online to anyone in the world. Unfortunately, these well-meaning open-access programs present a delicious opportunity for predators to exploit personal information. For example, in Hamilton County, Ohio, the Clerk of the Court maintains a comprehensive website that has advanced name search features on civil, criminal, and even parking violation cases freely available to anyone with Internet access.[180] The site requires no password or user fee, and the database is alarmingly user-friendly. To find all of the available records on someone, you simply search by name. Plastered on the Internet, any user—here in the United States or elsewhere—can browse through detailed court records kept on Ohio residents. Each file displays all of the publicly held information about a case, which occasionally includes SSN information, home addresses, and even financial disclosure forms.[181]

¶102 Of course, the problem with implementing well-meaning, open-access programs in cyberspace is that personal information belonging to local residents is suddenly hurled into a realm with no borders, accessible by anyone anywhere in the world. Left with no voice in deciding how their personal information is used, individuals whose information is freely exchanged must lie still and helplessly wonder about the underlying motives of an unfamiliar information-harvesting entity.

E. The European Experience

¶103 By contrast, in Europe, privacy is highly esteemed, not just by the law, but by its citizens. Privacy in Europe is anchored in fundamental human rights, and considered a matter of basic social protection. [182] By implementing the 1995 European Community Directive on Data Protection ("E.U. Directive"), the European Union ("E.U.") mandated that all fifteen E.U. Member States ensure that citizens have the right to access their data, fix incorrect information, remedy violations, and keep their information from being used for any marketing purpose without their permission.[183]

¶104 Placing a premium on individual choice, E.U. data protection laws define each citizen's basic legal right to control their personal information. Instead of presuming government and commercial enterprises have a right to collect and share personal information, the European approach tries to balance individual interests with legitimate commercial concerns to ensure a high level of data protection for all E.U. citizens. [184] More importantly, unlike

---

[179] *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002).

[180] Greg Hartman, Clerk of Courts, Hamilton County, Ohio, *at* http://www.courtclerk.org (last visited Mar. 21, 2004).

[181] *See* Liz Sidoti, *Revisiting Public Record Policies*, CBSNEWS.COM, Oct. 11, 2002, *at* http://www.cbsnews.com/stories/2002/10/11/tech/main525358.shtml (last visited Mar. 21, 2004).

[182] *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1347 (2000).

[183] Council Directive 95/46/EC of the European Parliament and of the Council, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) (Oct. 24, 1995) ("E.U. Directive"). Article 2(a) of the E.U. Directive broadly defines "personal data" as "any information relating to an identified or identifiable natural person." Article 2(b) defines data "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available. . . ."

[184] James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 83 (2003).

most privacy laws in the United States, the E.U. Directive applies essentially the same standards to both private sector and government databases.[185]

¶105 Ultimately, the challenge for U.S. policymakers will be to redefine privacy protections to meet the challenges of data exchange developments both here and abroad. At an international level, the modern privacy benchmark can be found in Article 12 of the 1948 Universal Declaration of Human Rights, which specifically protects both territorial and communications privacy: "No one should be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interferences or attacks."[186]

¶106 As it now stands, the geopolitical landscape has already questioned the feasibility of the varying standards of privacy protections between the United States and the European Union.[187] In an interconnected world, uniformity in privacy protections is the preferred choice. Perhaps, the obstacles to a more comprehensive approach to information privacy in the United States lie in our view of the appropriate function of government, and our notion of the private sector's role in ordering societal relationships.[188] Given the political history of the privacy debate in this country, some experts argue that no significant shift in U.S. policy is likely to occur until some crisis or highly publicized event forces us to look at the issue from a new perspective.[189]

IV. THE ROUGH ROAD AHEAD

¶107 At this critical stage in the Internet's sociopolitical development, we simply cannot afford to look the other way when it comes to developing sound Internet safety policies. If nothing else inflicts a sense of urgency for taking safety in cyberspace seriously, homeland security policymakers should realize that the Internet's global network could be used, not by the familiar juvenile hacker, but by a new breed of sophisticated adversary to attack our critical information systems.

¶108 As we grow more dependent on Internet technology to conduct our daily affairs, so does the likelihood that evil minds will one day target the central nervous system of our Information Age.[190] "We have a system that is fragile, that is vulnerable to sophisticated attacks . . . not to 14-year-olds, but to a sophisticated group, or nation-state, with multiple simultaneous attacks. It could lead to catastrophic damage to the economy, and, if done at a time of national security crisis, it could lead to catastrophic damage to our national defense."[191]

¶109 To complicate the situation, young people are the ones leading the way in using the Internet's hyper-evolving communications technology. Much more than their older counterparts, the younger generation of users embraces the Internet as a place to socialize.[192]

---

[185] *Id.* at 82-83.

[186] Universal Declaration of Human Rights, Article 12, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948, *available at* http://www.un.org/Overview/rights.html (last visited Mar. 21, 2004).

[187] *See* Jaikumar Vijayan, *EU privacy concerns on airline passenger data could cause rift with U.S.*, *EU commissioner warned that U.S. antiterror efforts could breach European privacy law*s, COMPUTERWORLD.COM, Sept. 5, 2003, *at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,84643,00.html (last visited on Mar. 21, 2004).

[188] *See* Nehf, *supra* note 184, at 90-91.

[189] *Id.* at 91.

[190] *See* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 ILL. J.L. TECH. & POL'Y 1, 27 (2002) ("At some future time, the United States will be attacked, not by hackers, but by a sophisticated adversary using an effective array of information warfare tools and techniques.").

[191] *Id.* at 55 (internal citations omitted).

[192] *See, e.g.*, *German Kids Go to Camp for Internet Addiction*, DW-WORLD.DE, Aug. 8, 2003, *at* http://www.dw-world.de/english/0,3367,1446_A_943281_1_A,00.html, (last visited Mar. 21, 2004) ("Much of the increase in Internet addiction is among children and young teenagers who spend increasing amounts of time playing computer games or surfing the Internet. And because Internet Addiction Disorder (IAD) has a very loose framework

For them, the Internet has moved cliques from the lunchrooms and lockers to live chats and online bulletin boards, thereby intensifying its reach and power. However, to socialize in cyberspace is to socialize on a whole new level of consciousness. The Internet has introduced users to a radically new social algorithm that imposes an unfamiliar ethical calculus. Lost in an idealistic environment designed to overcome personal inhibitions, Internet users of all ages can quickly forget the offline consequences of their online actions.

¶110 Often caught in the middle are parents of adolescent Internet users who seldom know where to turn for guidance. Stuck in this gray area of the law and society, school administrators often refrain from disciplining off-campus behavior and parents plead technological ignorance. In one message sent in November 2002 to WiredSafety.org, an anxious mother sought guidance after learning that her daughter was exchanging electronic messages with a stranger:

> *Recently, I caught my daughter talking to someone whose screen name I recognized from an artists chat room that I visit. I knew immediately that he was an adult and asked my daughter not to talk to him. Yesterday, I caught her in an IM with him again and saved it. Although there is nothing outright explicit in the conversation, it seemed very inappropriate. I am unnerved by this situation. I thought of contacting him directly and demanding he stop but I really want to stop him from talking to other children in this way. I think he is possibly a pedophile. What action should I take?*[193]

¶111 Inexplicably, although the United States is a leader in Internet technology, other countries have progressed much more quickly when it comes to promoting safety in cyberspace. Countries like the United Kingdom and New Zealand have effectively advanced forward-thinking strategies by creating independent Internet safety boards to develop nationwide initiatives.[194] These government-sponsored programs publish online safety materials for schools, foster international law enforcement alliances, fund online risk research, and give users a centralized authority in cyberspace for uniform guidance.

¶112 In 2002, the Education Department in the United Kingdom launched an innovative program for Internet users to learn safety skills. In one event held this year at the Kingwood City Learning Centre in London, schools hosted workshops for parents and children to become e-literate together. During an interview with BBC News, Schools Communications Technology Manager Doug Brown explained that "parents are obviously concerned with net safety issues and they tend to hear only about the problems and not the benefits. It is crucial that parents have an understanding of what the Internet is and find out about the value of e-learning."[195] These types of programs highlight the educational benefit of the Internet, while offering valuable safety resources in cyberspace for families.

¶113 We in the United States should do at least as much—if not more—along these lines. For too long, the Internet and global policy have evolved at starkly different paces. On the one hand, communications and software development companies cave to market forces in a rush to introduce new product features and woo anxious investors. On the other, policymakers put off enacting any legislative proposals that may impose additional administrative burdens so as to not upset their corporate constituents. This crippling imbalance has created an enormous gulf between user expectations and technology's true

---

of diagnosis and is yet to be recognized formally as a chronic psychological problem, it goes unaddressed by many parents. Even more have no idea that help is at hand.").

[193] E-mail sent to LegalEagles at WiredPatrol.org (Nov. 5, 2002) (copy on file with author).

[194] *See Online Child Safety Drive Launched*, BBC NEWS, Jan. 6, 2003, *available at* http://news.bbc.co.uk/1/hi/uk_politics/2629611.stm (last visited Mar. 21, 2004); NetSafe, New Zealand Internet Safety Group, *at* http://www.netsafe.org.nz/home/home_default.asp (last visited Mar. 21, 2004).

[195] *Children learn net skills with parents,* BBC NEWS, WORLD EDITION, Oct. 1, 2002, *available at* http://news.bbc.co.uk/2/hi/technology/2288620.stm (last visited Mar. 21, 2004).

potential. Consumers remain too vulnerable in cyberspace, and often hesitate before experimenting with the Internet's untapped potential to reach a global audience.

¶114 With this in mind, Kofi Annan, Secretary-General of the U.N., described the Internet as one of the most visible examples of the way information and communications technologies can contribute to economic growth on an international level. "But knowing that an instrument is powerful is not enough to ensure that it will be put to the best possible use. We need to understand how it works, and how and when it should be used, and find creative ways to put this knowledge into practice, disseminate it widely, and maximize its power."[196]

¶115 Given the stakes, policymakers should adequately support more comparative Internet safety policy projects that closely examine existing international efforts to combat dangerous activity in cyberspace, while exploring ways to protect users from foreseeable harm. By analyzing existing protections, government officials may then be better able to explore uniform codes of conduct for Internet users.

¶116 To permanently resolve these problems requires innovation, resources, and time. However, dealing head-on with user concerns about personal safety in cyberspace requires immediate attention. Ideally, the Internet will one day become a place where all gather to learn, shop, and interact peaceably within the comfort of our homes. But before the Internet can reach its full potential, we must first rethink safety, privacy, and security in a way that suits this virtual forum.

V. CONCLUSION

¶117 In sum, U.S. policymakers should rethink privacy and consumer safety in cyberspace. Identity theft is on the rise because consumers have no control over their own personal information. Such scams illustrate the serious economic consequences that stem from lax information-sharing policies of banks, credit card companies, landlords, employers, and online services. Any system in which consumers do not have a choice about how their information is collected, shared, or used, is one in dire need of renovation. Florida Law Enforcement Special Agent Robert Ivey, an officer with twenty years of experience, predicts that "identity assumption and takeover is becoming the most serious non-violent crime challenge that America faces."[197]

¶118 By contrast, cyberstalking tactics uncover a more personal threat, and the damage it can exact on a victim's physical and psychological well-being. To some, cyberstalking is a necessary consequence of taking our daily activities from the physical realm into a virtual domain. The Internet's anonymous nature and borderless domain gives cyberstalkers free rein to employ creative terror tactics. Policymakers and law enforcers around the world have yet to seriously explore viable legal mechanisms to deal with cyberstalking. Left unaddressed, officials will remain unable to reasonably ensure personal safety online, faced with the formidable technological obstacles to identifying, locating, and arresting cyberstalkers.

¶119 At the heart of identity theft and cyberstalking lies information privacy protection. With the increase in Internet use comes a new sense of personal comfort. But, as more of us become more comfortable with using the Internet for everyday activities, we become more vulnerable to new types of privacy invasions. Indeed, with all the personal information available in the public domain, the once obvious line between public and private realms becomes difficult to discern.

---

[196] U.N. CONF. ON TRADE AND DEV., E-COMMERCE AND DEVELOPMENT REPORT, *supra* note 8.

[197] *Protecting Privacy and Preventing Misuse of the Social Security Number, 2000: Hearings on H.R. 4857 Before the Subcomm. on Soc. Sec. of the House Comm. on Ways and Means*, 106th Cong. (2000) (statement of Robert W. Ivey, Special Agent, Florida Department of Law Enforcement).

¶120 In the end, this much is true: Before any of us can truly be free in cyberspace, we must first be safe. The steps we take—or fail to take—at this critical stage could forever determine the role that the Internet will play in our future.