A United States Perspective on the Ethical and Legal Issues of Spyware

Janice C. Sipior
College of Commerce & Finance
Villanova University
Villanova, PA 19085 USA
+1-610-519-4347
janice.sipior@villanova.edu

Burke T. Ward
College of Commerce & Finance
Villanova University
Villanova, PA 19085 USA
+1-610-519-4375
burke.ward@villanova.edu

Georgina R. Roselli
College of Commerce & Finance
Villanova University
Villanova, PA 19085 USA
+1-610-519-4347
georgina.roselli@villanova.edu

ABSTRACT
Spyware is regarded as the largest threat to internet users since spam, yet most users do not even know spyware is on their personal computers. Ethical and legal concerns associated with spyware call for a response. A balance must be found between legitimate interests of spyware installers, who have obtained informed consent of users who accept advertisements or other marketing devices, and users who are unwitting targets. Currently, there is not widespread awareness or understanding of the existence of spyware, its effects, and what remedies are available to defend against it. For industry sectors subject to data collection and protection laws, spyware results in unintentional noncompliance. This paper examines the ethical and legal issues of spyware from a United States perspective. First, the increasing prevalence of spyware is discussed. Various types of spyware are then overviewed. Ethical and legal concerns, including privacy invasion, surreptitious data collection, direct marketing, hijacking, and trespass are discussed. Finally, various methods of responding to spyware, including approaches by consumers, industry, and the U.S. government, are addressed, calling for a need to resolve escalating concerns of users while balancing the beneficial use of spyware as a legitimate marketing tool.

Categories and Subject Descriptors
K.5.1 [**Legal Aspects of Computing**]: Hardware/Software Protection – *Proprietary rights.*

General Terms
Management, Security, Legal Aspects.

Keywords
Spyware; Privacy; Trespass; Ethics; Law

1. INTRODUCTION
Computer users are threatened by stealth invaders, in the form of spyware, which gather users' personal information and may also disrupt computer operation. Spyware is regarded as the largest threat to internet users since spam, yet most users do not even know spyware is on their personal computers (PCs) [32].

ICEC'05, August 15–17, 2005, Xi'an, China.

While information concerning user characteristics and preferences may be used beneficially to improve product and service offerings, the surreptitious nature of its acquisition coupled with no indication of its intended use may raise ethical and legal issues regarding its acceptability. Ethically, spyware installers have an obligation to users to obtain informed consent for the collection and use of personal information. However, in the commercially competitive environment of electronic commerce, information gathering may be undertaken without users' knowledge or permission.

For industry sectors which are subject to data collection laws, "spyware can be an unwitting avenue to noncompliance" [9]. Within the United States (U.S.), federal statutes govern the use and disclosure of personally identifiable information within various industry sectors [26]. For example, the Financial Services Modernization Act of 1999, informally known as the Gramm-Leach-Bliley Act (GLBA), protects the privacy of consumer information in the financial services industry. The Sarbanes-Oxley Act of 2002 (SOX), intended to increase corporate responsibility, requires financial institutions to protect the privacy of customer records and information. In the health care industry, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 provides privacy protection for patients' information. Should stealth spyware arrive, industry is confronted with the risk of violating legislation protecting the security and privacy of proprietary information and systems.

This paper examines ethical and legal issues of spyware from a U.S. perspective. First, the increasing prevalence of spyware is discussed. The various types of spyware are then overviewed. Ethical and legal concerns of spyware, including privacy invasion, surreptitious data collection, direct marketing, hijacking, and trespass are discussed. Finally, the various methods of responding to spyware, including approaches by consumers, industry, and the U.S. government, are addressed, calling for a need to resolve escalating concerns of users while balancing the beneficial use of spyware as a legitimate marketing tool.

2. THE INCREASING PREVALENCE OF SPYWARE
"Spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to consumers" [20]. Spyware includes "[a]ny software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes" [20]. The definition is so broad that it may cover software that is beneficial and benign, or software that has poorly written, inefficient code [21]. The Center for Democracy and

Technology, a policy research group, has proposed that software which hijacks web traffic, tracks internet users without their knowledge and consent, and is not easily removable should be considered spyware.

As presented in Table 1, an audit of over 4.6 million PCs to date found 116.5 million instances of spyware, averaging 25 per PC [17]. Over 7,000 spyware programs are estimated to be running on millions of corporate and personal computers [13]. Gartner Research estimates that over 20 million users have spyware on their PCs [5]. According to a survey of home PC users conducted by America Online, spyware is present on 80% of home PCs, while about 90% of those with spyware are neither aware of what it is or of its presence [29]. According to Microsoft, spyware is responsible for half of all PC crashes [32]. Indicative of the increasing disruption users experience, Dell Tech Support Services reports spyware complaints are the most common reason consumers contact Dell [33], with about 20% of calls related to spyware or viruses, up from 2% eighteen months earlier [4].

Table 1. Instances of Spyware

	Number of Instances of Spyware Found				
Type	**1st Quarter**	**2nd Quarter**	**3rd Quarter**	**4th Quarter**	**To Date**
Adware	3,558,595	7,887,557	5,978,018	6,971,086	24,395,256
Adware Cookies	14,799,874	27,868,767	22,327,112	25,598,803	90,594,556
System Monitor	122,553	210,256	154,878	272,211	759,898
Trojan Horse	130,322	236,639	148,214	254,155	769,330
Total	18,611,344	36,203,219	28,608,222	33,096,255	116,519,040

Source: Earthlink, 2005

3. TYPES OF SPYWARE

Various types of spyware have been identified including adware cookies, adware, trojan horses, and system monitors. As shown in Table 1, adware cookies are the most prevalent form, representing 77.8% of instances of spyware [17].

3.1 Adware Cookies

Adware cookies are files containing information about a user's website interaction, which can be exchanged between the website and the user's hard drive. Cookies were originally intended for innocuous purposes such as keeping track of items in an online shopping cart, simplifying the log-in process, and providing users with customized information based on stated interests [23]. However, cookies can be used to create profiles of user's online behaviors without the user's knowledge or consent.

3.2 Adware

Direct marketers use adware to track users' online behavior, with or without users' consent. Detailed target market profiles are compiled to deliver specific offerings customized for individual users. These advertisements can take the form of pop-up or pop-under ads, web banners, redirected webpages, and spam email.

3.3 Trojan Horses

Trojan horses, or Remote Administration Trojans (RATs), are a malicious form of spyware, which takes control of a user's computer by installing itself with a download and taking directions from other computers it contacts via the internet. Trojans can turn a PC into a spam proxy or use Microsoft Outlook email as if it were a browser to allow for a torrent of pop-up ads [16]. Trojans may also be designed to steal data or damage files.

3.4 System Monitors

System monitors, also referred to as keystroke loggers, surreptitiously collect data from user interaction while shopping or banking online and locally while using software such as spreadsheets or videogames. This data can be transmitted back to the spyware installer, shared with other businesses such as marketers, or sold to data consolidators.

4. ETHICAL AND LEGAL ISSUES OF SPYWARE

The controversy surrounding spyware results from ethical and legal concerns associated with its distribution and capabilities. The issues, discussed below, include privacy invasion, surreptitious data collection, direct marketing, hijacking, and trespass.

4.1 Privacy Invasion

Privacy is a major concern raised by spyware [11], based mainly upon the potential for intrusions into a user's computer resources for surreptitious data collection, dissemination of an individual's private information, and uninvited direct marketing. Without knowingly providing permission for the installation of spyware, the user is likely to see spyware as a violation of privacy.

Legal protection of privacy within the U.S. remains unclear. Recognition of privacy rights within the U.S. occurred in the late 1800's [34]. Almost a half century ago, privacy was recognized as, in part, a spiritual issue, the unprivileged invasion of which is an affront to individuality and human dignity [6]. Is spyware such an unethical affront to individual human dignity, to be afforded legal protection? Currently, privacy protection in the U.S. is a complex amalgam of federal and state constitutions, statutes, and regulations. The, reasonableness of a user's expectation of privacy differs depending on whether the claim is made under constitutional, common, or statutory law.

4.2 Surreptitious Data Collection

Spyware can surreptitiously capture personal information stored or typed into a PC. Information obtained can be transmitted to the spyware installer and partners for marketing or fraudulent purposes. These sites can "phish" for data while users surf, bank, and make purchases, or promote pornography, gambling, or fraudulent schemes. An investment broker reportedly lost $540,000 after installing a phony market analysis program that transmitted his account information to hackers [1]. Other uses may evolve, such as stealing corporate secrets from Word and Excel documents [27] or recording telephone conversations [24].

A novel form of spyware is the "Backdoor Santa," a stand-alone program that gathers user information. A popular example is a novelty cursor. Using a Globally Unique IDentifier (GUID), issued when the program is downloaded, the provider's servers are contacted to record logs of cursor impressions, the identity of referrers, and other information. The data collected is purchased by clients to inform them of

how many users have customized cursors obtained from specific sites [31].

Comprehensively informing users of what data is collected when and for what purpose, the impact of activities on computer performance, and being presented with the opportunity to grant permission may remove the stealth reputation of such activities.

4.3 Direct Marketing

Adware servers pay software companies to include spyware with legitimate software to gather user information. Once installed on the user's computer, user information is sent to the advertiser which serves the targeted ad. Interactive media expenditures are projected to grow 18.9% annually, reaching US$5.0 billion in 2006 [15], raising concerns about its acceptability.

Adware may be used beneficially to improve offerings to consumers. For example, by determining what advertisements a website visitor has already seen, only new ads are presented during future visits. This seems rather innocuous and perhaps even desirable. However, if used to promote pornography, gambling, or fraudulent schemes, adware becomes a questionable medium. Although adware applications are usually disclosed, in the End User Licensing Agreement (EULA) of software it accompanies, and can be uninstalled from the user's system [33], such disclosures may not be read. Without explicit user permission, the user is likely to object to the delivery of adware.

4.4 Hijacking

Spyware, such as trojan horses, can persistently disallow the user control over his computing resources [11]. Most users are not aware of the depth of penetration into their systems [28]. The browser's home page, default search engine, bookmarks, and toolbars can be changed to persistently present a competitor's web site or a look-alike site. Mistyped URLs can be redirected to pornographic sites and pop-up advertising can be presented. Websites may be launched without any action by the user. Dialers can use a telephone modem to dial into a service, such as a pornographic 900 number, for which the user is then billed [24]. System settings can be modified. For example, the auto signature can be reset; uninstall features can be disabled or bypassed; and anti-virus, anti-spyware, and firewall software can be modified. Hijacking is particularly offensive due to its persistent nature.

4.5 Trespass

Spyware usually arrives uninvited from file-sharing services as hidden components bundled with desired downloads, but can also be included with purchased software. Spyware can masquerade as a legitimate plug-in or pose as a browser help object, such as a toolbar. Users may unwittingly consent and accept spyware by agreeing to, but not reading, the EULA. Spyware can also be distributed in a variety of stealth ways. For example, a "drive-by download" starts a download process when a user visits a website or clicks on a web ad. Users may also be tricked into installing spyware. A message box may appear saying, "To install this program, click 'No'" prompting a user to unknowingly click for installation. Spyware can also covertly install other programs as part of an "auto-update" component. New security vulnerabilities are created by including capabilities to automatically download and install additional programs.

Once installed, spyware utilizes the user's own resources. Monitoring or hijacking can significantly slow computer performance. Random error messages, pop-up ads, or a surprise browser homepage or toolbar may appear. Common keys, such as tab, may no longer function. The transmission of user information gathered by spyware uses valuable bandwidth and threatens the security of computers and the integrity of online communications. Even with the use of anti-spyware software, removal can be impossible [7]. Knowledge of how to manipulate the Windows registry is required for persistent spyware. Diagnosing compromised system performance and removing spyware places a substantial burden on users or corporate support centers [11].

Uninvited stealth spyware could arguably be considered trespassing. Applying common law, this unauthorized invasion is called trespass to chattels, i.e., personal property. This is a legal remedy for an individual, not a governmental remedy that protects society generally. Governmental remedies, such as actions by the Federal Trade Commission (FTC), are discussed later, in the section addressing U.S. Legislation.

According to the Restatement (Second) of Torts, § 217, a trespass to chattel may be committed by intentionally

(a) dispossessing another of the chattel, or

(b) using or intermeddling with a chattel in the possession of another.

Although not yet been applied in any legal action, it is arguable that a user is dispossessed, not physically of course, but at least constructively, by the uninvited spyware. At a minimum, the spyware installer is using and intermeddling with the user's possession through unauthorized data collection, control of his browser, webpage redirection, search engine substitution, pop-up ads, and hijacking. Possession is defined in § 216 as "physical control… with the intent to exercise such control on his own behalf, or on behalf of another." Spyware clearly interferes with control, and therefore should be subject to legal action.

If the unauthorized installation of spyware is actionable as a trespass to chattel, the installer should be liable to the injured party. The Restatement at § 218 states that "[O]ne who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

(a) he dispossesses the other of the chattel, or

(b) the chattel is impaired as to its condition, quality, or value, or

(c) the possessor is deprived of the use of the chattel for a substantial time, or

(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest."

Depending on the characteristics and purpose of the spyware, at least one, and possibly all, of these consequences will be present.

5. RESPONSES TO SPYWARE

The approaches to reduce unwanted spyware include user initiatives, technological approaches, industry self-regulation,

and legislation, as shown in Table 2. None of these approaches alone has been effective. Rather, battling spyware requires a combination of these approaches [11].

Table 2. Responses to Spyware

User Initiatives
1. Vigilance
2. Alternate Internet Browsers
3. Hosts File and Proxy Automatic Configuration (PAC) File
Technological Approaches
1. Anti-Spyware Software
2. Firewalls
3. Spyware Blockers
Industry Self-Regulation
1. FTC endorses the use of self-regulation
U.S. Federal Legislation Pending
1. Internet Spyware (I-SPY) Prevention Act of 2005
2. Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)
State Legislation
1. Utah Spyware Control Act
2. California Computer Spyware Act

5.1 User Initiatives

Users may undertake some defense against spyware through vigilance in interacting with the internet and properly managing computing resources. Users may install and use alternate internet browsers not targeted by spyware. Additionally, the Windows Hosts file or the Proxy Automatic Configuration (PAC) file in the browser may be used to block access to websites known for spyware.

5.1.1 Vigilance

First and foremost, users need to be vigilant in downloading files. Before installing any software, a user should carefully read the EULA. Ethically, spyware bundled with the download should be disclosed in this "clickwrap" agreement. Software for purchase may also contain spyware [14]. The FTC [19] warns against installing software without knowing exactly what it is.

Users can take additional actions to reduce the potential for spyware [19]. Avoid peer-to-peer networks, which offer downloads containing spyware intended to generate revenues from advertising with which it is packaged, and visit only known websites to minimize "drive-by" downloads. Do not use instant messengers or shopping or search helpers. Run a virus check on unfamiliar files. Update operating system and web browser software to obtain "patches" to close holes that spyware could exploit. Set the browser security setting to medium or high to detect download attempts. Turn off the PC when not in use.

5.1.2 Alternate Internet Browsers

Microsoft's Internet Explorer (IE) is the standard internet browser, used by 95% of all web users [18]. Recently, an onslaught of malware has exposed vulnerabilities to IE. Users can download the Windows XP Service Pack to correct security issues, but there is another option. Alternatives, such as Mozilla's Firefox, are competent browsers that are free to users. Such alternative browsers are currently more secure than IE due, in part, to the fact that these alternate browsers are smaller targets for malware authors [18].

5.1.3 Hosts File and Proxy Automatic Configuration (PAC) File

Users may choose to utilize two alternatives already present within their PCs [8] to create a list of websites, or even webpages, to not visit, thereby blocking access to websites known for spyware. One alternative is the Windows Hosts file, a text file stored under the Windows folder. When a web address, called a domain name, is typed into a browser, the browser first checks the Hosts file. The central Domain Name Services (DNS) server is then contacted to look up the numeric equivalent of the web address, the Internet Protocol (IP) address, necessary to locate the website to be displayed. If the Hosts file contains an IP address for the domain name to be visited, the browser never contacts the DNS. The Hosts file can be edited in Notepad to enter a list of known spyware sites and redirect them to: 127.0.0.1 localhost, which is the IP address the computer uses to refer to itself, the local host. This effectively blocks requests made to undesirable sites because the domain name of such websites will point to the local host.

Alternatively, end users may choose to use a feature in their browser called Proxy Automatic Configuration (PAC) file to selectively block individual webpages. The PAC file is written in JavaScript, introduced with Netscape Navigator 2.0 in 1996 [25]. The browser evaluates a JavaScript function for every Uniform Resource Locator (URL), i.e., webpage, to be displayed. Like the Hosts file, the JavaScript function in the PAC file blocks access by redirecting the requested webpage to the local host. Hosts files however, can only block entire websites, while PAC files can block addresses of individual webpages within a site.

5.2 Technological Approaches

Technological approaches include anti-spyware software, firewalls, and spyware blockers. The market for anti-spyware software is still small, with $10-$15 million in sales, compared to the $2.2 billion anti-virus software industry. Effective anti-spyware software should identify the spyware threat, provide an explanation of the threat, and allow the user to decide what to remove. To date, no anti-spyware utility can provide an impenetrable defense [12]. Attracted to the potential to generate advertising revenue, professional programmers continue to refine spyware to make it difficult to identify and remove. Therefore, at least two anti-spyware tools should be used, as the first may not detect something that another tool does. Further, every network or PC that accesses the internet should have its own firewall. Defensive spyware blocker software can also detect and stop spyware before it is installed.

5.3 Industry Self-Regulation

Most reputable technology providers feel that adherence to the following five principles is crucial for adware providers [33]:

1. Clear and prominent notification presented to the user prior to downloads or data collection. Additionally, the EULA contains such notification.

2. The user has the opportunity to accept the terms of the application for both access to the user's PC and to any communications between a user's PC and the internet.

3. Easy removal procedures to uninstall unwanted applications.

4. Clear branding of pop-up windows to identify the ad's source.

5. Adherence to all application laws and best business practices for internet business.

The FTC is currently endorsing the use of self-regulatory measures as opposed to the introduction of legislation [20, 33].

5.4 U.S. Legislation

The U.S. federal government is investigating the effects and legitimacy of spyware, with the FTC leading the charge. While legislation has been proposed at the federal level in the Senate and House of Representatives, some states have already imposed regulations. Spyware has not yet caused widespread public outcry because most users are unaware that their systems have been compromised [30].

5.4.1 Federal Trade Commission

The FTC currently has legal authority to take actions, both civilly and criminally, against spyware installers. Civil action would be brought under the FTC Act §5 to regulate "*unfair or deceptive acts or practices.*" Criminal action would be brought under the Computer Fraud and Abuse Act to provide remedies against whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." The FTC conceded that if the spyware infiltration continues, there could be "loss in consumer confidence in the Internet" [22].

5.4.2 Pending Federal Legislation

The Internet Spyware (I-SPY) Prevention Act of 2005 [2], introduced in the House on February 10, 2005, amends the Federal criminal code to discourage spyware. This bill prohibits the intentional access of a protected computer, without authorization, to install spyware to transmit personal information with the intent to defraud or injure an individual or cause damage to a protected computer. Penalties of fines, or imprisonment of up to five years, are included. In addition, $10 million would be provided annually for years 2006 through 2009 to the Justice Department for enforcement. This bill has been referred to the House Committee on the Judiciary.

The Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) [3] was introduced in the House on January 4, 2005. This bill is intended to protect internet users from unknowingly transmitting personally identifiable information through spyware. Activities relating to spyware which are prohibited include taking control of another PC, modifying settings on another PC, collecting personally identifiable information via keystroke loggers, and persuading the user to install spyware or prevent efforts to block spyware. The penalty for violating any of these prohibitions includes a civil fine of up to $3 million. On March 9, 2005, the House voted unanimously that the bill be amended.

5.4.3 State Legislation

On March 23, 2004, the Utah Governor signed the nation's first anti-spyware legislation. The Spyware Control Act prohibits the installation of software without the user's consent, including programs that send personal information. Under this law, only businesses are given the right to sue. This measure has yet to be enacted however, as litigation from the adware firm WhenU has resulted in a preliminary injunction against it.

In California, the Consumer Protection Against Computer Software Act became effective January 1, 2005, this law prohibits the installation of software which deceptively modifies settings, including a user's home page, default search page, or bookmarks, unless notice is given. Further, it prohibits intentionally deceptive means of collecting personally identifiable information through keystroke-logging, tracking web surfing, or extracting information from a user's hard drive. A consumer may seek damages of $1,000, plus attorney's fees, per violation. Iowa, New York, and Virginia are currently considering anti-spyware measures.

6. CONCLUSION

Ethical and legal issues associated with spyware call for a response. The form of that response will ultimately be determined by users themselves through their assessment of the ease and effectiveness of the various approaches to battling spyware. Will user protests ultimately be so strong as to lead to legal legislation? While the concerns associated with the presence of spyware are clear, legislating spyware is difficult because the definition of spyware is vague. Passage of legislation has been slow because broad legislation could prohibit legitimate practices and stifle innovation. Protecting consumers' concerns has to be carefully balanced against the beneficial use of spyware as a legitimate marketing tool. Currently, there is not widespread awareness or understanding on the part of users as to the existence of spyware, its effects, and what remedies are available to defend against its installation or removal. As the prevalence of spyware continues to increase, escalating concerns of users regarding the acceptability of spyware will ultimately drive a resolution in balancing the legitimate interests of spyware installers with those of users.

7. REFERENCES

[1] Bugged by spyware? (2003). *Database and Network Journal*, 33(16): 22-23.

[2] Internet Spyware (I-SPY) Prevention Act of 2005 (HR 744.IH), http://thomas.loc.gov/cgi-bin/query/D?c109:1:./temp/~c109XoBJWT::, visited March 15, 2005.

[3] SPY ACT (HR 29.IH), http://thomas.loc.gov/cgi-bin/query/ D?c109:2:./temp/~c109XoBJWT::, visited March 15, 2005.

[4] Bank, D. (2004). What's that sneaking into your computer? *Wall Street Journal*, 26 April: R1.

[5] Batchelar, R. (2004). Don't be snookered by sneaky spyware, *Australasian Business Intelligence*, March: 14c.

[6] Bloustein, E. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYU Law Review*, 39: 962-1007.

[7] Borland, J. (2003). Spike in "spyware" accelerates arms race, *CNET News.com*, 24 February: http://news.com.com/2009-1023-985524.html.

[8] Canter, S. (2004). No-cost ad blocking; PAC files are even better than HOSTS files for blocking Web site ads, *PC Magazine*, 23(19): 70.

[9] Carlson, C. (2004). Spyware beware, *eWeek*, 21(26): 33.

[10] Carroll, S. (2004). How to avoid spyware, *PCMagazine*, 23(4): 79.

[11] Center for Democracy & Technology (2003). Ghosts in our machines: Background and policy proposals on the 'spyware' problem, November. www.cdt.org/privacy/031100spyware.pdf, visited October 25, 2004.

[12] Clyman, J. (2004). Antispyware: Adware and spyware are a growing nuisance and threat, *PC Magazine*, 23(13): 82.

[13] Coggrave, F. (2003). Is someone using spyware to monitor how your employees are using their computers? *Computer Weekly*, 11 November: 38.

[14] Delaney, K.J. (2004). Videogame makers borrow TV's tactics for selling ads, *Wall Street Journal*, 18 October: B5.

[15] Direct Marketing Association. (2002). Economic impact: U.S. direct & interactive marketing today executive summary– 2002: Interactive marketing: http://www.the-dma.org/cgi/registered/research/libres-ecoimpactinteractive. shtml.

[16] Duntemann, J. (2004). Degunking your PC, *PC Magazine*, 23(14): 60.

[17] Earthlink (2005). Earthlink spy audit, http://www.earthlink.net/spyaudit/press, visited March 15, 2005.

[18] Edvalson, R. (2004). Commentary: Explorer's pitfalls aren't easy to avoid, but choices exist, *The Idaho Business Review*, 2 August: 1.

[19] FTC (2004a). FTC consumer alert: Spyware, October 2004, http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm, visited October 17, 2004.

[20] FTC (2004b). Prepared statement of the Federal Trade Commission before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, United States House of Representatives, Washington, D.C., April 29, 2004, http://www.ftc.gov/os/2004/04/040429spywaretestimony.htmvisited October 18, 2004.

[21] FTC (2004c). Conference: Monitoring software on your PC: Spyware, adware, and other software, April 19, 2004, www.ftc.gov/bcp/workshops/spyware/index.htm, visited October 18, 2004).

[22] FTC (2004d). Spyware poses a risk to consumers, April 29, 2004. http:www.ftc.gov/opa/2004/04/spywaretest. htm, visited October 25, 2004.

[23] Furger, R. (2000). Who's watching you on the web? *PC World*, March: 33.

[24] Gilmour, K. (2004). Destroy all spam and spyware, *Internet Magazine*, February: 24-33.

[25] LoVerso, J.R. (2004). Bust banner ads with proxy auto configuration, www.schooner.com/~loverso/no-ads, visited October 28, 2004.

[26] Norian, P. (2003). The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond, *Catholic University Law Review*, Volume 52, Number 803, p. not available.

[27] Radcliffe, D. (2004). Spyware: How to fight back against insidious attacks from cookies gone bad, *Network World*, 21(4): 51.

[28] Rensberger, D. (2002). We are not alone: Spam and spyware, *Searcher*, April: 20-26.

[29] Roberts, P. (2004). Your PC May Be Less Secure Than You Think, *IDG News Service*, October 25, http://www.pcworld.com/news/article/0,aid,118311,00.asp, visited March 15, 2005.

[30] Rubenking, N.J. (2004). 11 signs of spyware, *PC Magazine*, 23(4): 79.

[31] Smith, G. (1999). Tracking brawl: Is Big Brother watching you online, or are you just paranoid? *ABCNews.com*, 17 December.

[32] Sullivan, A. (2004). Spyware emerges as new online threat, *Boston Globe* 19 April: C2.

[33] Urbach, R. R. and G.A. Kibel (2004). Adware/spyware: An update regarding pending litigation and legislation, *Intellectual Property and Technology Law Journal*, 16(7): 12 +

[34] Warren, S.D. and L.D. Brandeis (1890). The right of privacy, *Harvard Law Review*, December: 193-220.

[35] Ding, W., and Marchionini, G. *A Study on Video Browsing Strategies.* Technical Report UMIACS-TR-97-40, University of Maryland, College Park, MD, 1997.

[36] Fröhlich, B. and Plate, J. The cubic mouse: a new device for three-dimensional input, *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI '00)* (The Hague, The Netherlands, April 1-6, 2000). ACM Press, New York, NY, 2000, 526-531.

[37] Lamport, L. *LaTeX User's Guide and Document Reference Manual.* Addison-Wesley, Reading, MA, 1986.

[38] Sannella, M. J. *Constraint Satisfaction and Debugging for Interactive User Interfaces.* Ph.D. Thesis, University of Washington, Seattle, WA, 1994.