Journal of International Technology and Information Management

Volume 17 | Issue 2 Article 3

2008

The Voyeur among Us: Navigating Around the Global Spyware Epidemic

Daniel B. Garrie
CRA International, New York, NY

Liane R. Komagome
CRA International, Houston, TX

The Voyeur among Us: Navigating Around the Global Spyware Epidemic

Daniel B. Garrie
CRA International, New York, NY

Liane R. Komagome
CRA International, Houston, TX

ABSTRACT

Spyware poses a serious threat of privacy infringement to unassuming internet users across the globe. Existing European legislation attempts to protect end-users from unethical review and use of their personal data. Outlawing spyware technology and strengthening the legal consent requirement for data-mining may offer end users additional assurances that their privacy rights are upheld, as well as more tangible shelter from the existing spyware epidemic. These proposed solutions, however, will only create successful safe havens for internet users by obtaining international buy-in.

INTRODUCTION

With today's rapid rate of technological advancement, it is imperative that judicial systems around the world involve their legal systems to address the global problem of spyware. Because digital privacy is not limited to a specific geographical boundary, protection of privacy must be regarded as a global issue. As society world wide becomes more dependent on technology, the risk surrounding its misuse increases exponentially and demands greater awareness and action by the average citizen.

Spyware, whether in Europe or the U.S., is flourishing. A recent International Data Corporation (hereafter "IDC") survey identified spyware as the fourth greatest threat to enterprise security (Gordan, 2005). An AOL/National Cyber Security Alliance (NCSA) Online Safety Study also recently reported that 80 percent of scanned computers contain a variety of spyware or adware (Gordan, 2005). Thus, we must address the existence of spyware and its ever-growing, evolving nature due to our computer-driven society.

Despite the strict data processing protection laws adopted by the European Union (hereafter "E.U."), little has been done to protect European Internet users from spyware (Levy & Stone, 2005). Left largely unchecked by legal remedies, spyware has infiltrated and overrun personal computers worldwide. This paper expounds the threat of spyware in light of its technical capabilities, analyzes how spyware violates existing European law, and proposes both statutory and non-statutory methods to successfully defeat this parasite (For a description of losses due to identity theft and the potential liability of those stealing the information, see Byers, 2001).

TECHNOLOGICAL OVERVIEW OF SPYWARE

Understanding spyware requires the realization that any connection to a site on the World Wide Web [hereafter "Web"] is not passive and the visitor does not wander around invisibly. Connecting to the Web is not like opening a book in the library and looking at its contents. While the person accessing the Web is gathering information from the site, the site knows the visitor is there, is monitoring the visitor's actions and has varying levels of access, by the visitor's invitation, to that visitor's computer. One of the earliest forms of this active interaction was cookie technology.(Gordon, 2005). Most users find cookies beneficial because they "[e]liminate the need to repeatedly fill out order forms or re-register on Web sites" (Gordon, 2005). For instance, with passwords being increasingly difficult to remember, some sites that require user names and passwords place cookies on the hard drive so that the user has the option to log-in automatically when visiting.

The reality is, however, that many businesses seek more competitive advantages, and, consequently, have developed a variety of legitimate and illegitimate technologies to enhance their market advantage. Some modifications that

transform legitimate cookie technologies into illegitimate ones include data miners that actively collect information, dialers that change the computers dial-up networking, worms that create self-replicating viruses, and hijackers that hijack a user's home page are (Lavasoft, Spyware & Harmful Technologies, 2005).

Spyware Defined

Spyware is generally defined as software that, once installed on a person's computer (usually without consent), collects and reports in-depth information about that end-user (Gordan, 2005). Spyware is the progeny of clickstream data or cookie based data mining technology (Brandt, 2000). These technologies are viewed as instrumental to the operation of the global information society. To demonstrate this expansive reliance on cookie technologies, the reader need only view the cookies stored on any personal computer.[1] The intertwined nature of spyware to other data mining technologies makes regulation a very delicate and difficult process. Most web portals would be severely limited, if not rendered useless, in the absence of spyware-like technologies. A sampling of Web sites that would not operate if such technology was prohibited is as follows: www.yahoo.com; www.google.com; www.wamu.com; www.schwab.com; www.ibm.com; (U.S Dep't of Commerce, 2000) and adjoining these web sites are a slew of intranet and Web applications that utilize cookies and clickstream data for authentication.

Spyware is capable of gathering a wide range of information, including web-surfing habits, each and every keystroke, e-mail messages, credit-card information, and other personal information on users' computers (Adelman, 2005). In the world of technology, "Spyware" is the umbrella term under which numerous technologies, both legal and malicious, fall including: adware (Hagerty & Berman, 2003); trojans; hijackers (Wilson, 2005); key loggers (Schultz, 2003); malware (Carfarchio, 2002); and, dialers (Wilson, 2005). While each of these technologies has its own unique behavior, for the most part they are all installed without a user's informed and explicit consent, and tend to extract varying degrees of personal information, usually without that end-user's consent (Spiror, 2005). For instance, Trojan spyware operates with a focus on password-stealing using a "trojanized" piece of software to grab passwords, either directly from the keyboard or while in transit over the network, has been implemented many times on a raft of different platforms, which is installed without the user's consent (Wilson, 2005).

Spyware operates in relative secrecy, gathering end-user information without the end-user's consent or knowledge. When spyware successfully installs it is difficult to remove because it embeds itself within the system and uses various techniques to detect and replace various files that are integral to the operation of the user's machine, so if a user rips out one or two parts, the undetected parts will come in and replace the files that were removed (Wilson, 2005). The outcome is that although the user is aware that spyware is installed, it is difficult for the user to remove, even when utilizing spyware removal technology (Schultz, 2003). Spyware blurs the existing fuzzy line between a malicious virus and an aggressive Internet marketing tool. Spyware, however, can monitor more than just the web pages an Internet surfer visits (for example, see Urbach & Kibel, 2004); it is able to access the end-user's electronic file system (Prostic, 2004), e-mail system, web pages viewed, and any other information the end-user accesses on the machine that is not encrypted (Volkmer, 2004).

While valid commercial uses for spyware exist, its primary purpose is to spy and to gather information by invading a user's protected digital space (Gibson, 2005), unbeknownst to the end-user (Foster, 2002), and to relay it to a third party. For instance, a malicious spyware application might "pop up" a dialog box that warns the user of a problem with his or her account only to redirect that person to a look-alike site, which then acquires personal financial resources (Krause, 2005). As Krause (2005) points out generally, malicious spyware tends to be financially motivated, distinguishing itself from past viruses/malware.

TWO TYPES OF SPYWARE

Spyware, once it is installed on an end-user's machine, can be cataloged in one of two ways: (1) software-enabled installation of spyware via shareware applications; and, (2) web-enabled installation through a user's browser. This distinction is drawn because spyware's delivery and installation mechanisms can be categorized as either software-enabled or web-enabled spyware.

Software Enabled Installation of Spyware via Shareware

As Moshchuk,T., Bragin, T., Gribble, S. and Levy H (2005), researchers from University of Washington Dep't of Computer Science, point out software-enabled spyware installs itself by way of attaching itself to shareware software, such as Kazaa (http://www.kazaa.com) to which spyware code has been attached to several hundred million machines. Commonly these software programs are embedded within a DLL (Dynamic Link Library) that the intruder can manipulate at a later date (Moshchuk, 2005). On average, such spyware has 93 components, making the process of removal, even for a knowledgeable technical person, an arduous and daunting, if not impossible, task (Moshchuk, 2005). Software-enabled spyware that relies on this attachment mechanism for installation has been coined "piggy-backed spyware" (Moshchuk, 2005).

The majority of software-enabled spyware programs fall within the "piggy-backed spyware" installation method. Once the spyware is installed it remains hidden from the user, (N. Leibowitz, public presentation, 2003), and because, the user consented to it's installation via the shareware application End User License Agreement (hereafter "EULA"), it does not violate black-letter law by transmitting data to third-parties (N. Leibowitz, public presentation, 2003). For instance, spyware is frequently in e-cards, which a commercial Trojan spyware are E-cards: romantic, joke and others with which ensnare a victim (Blakley, Garrie & Armstrong, 2005). This E-card spyware can be used to spy on unsuspecting parties; all that is needed to install the spyware is the email address of the target. (Simpson, 2003) It is able to snoop remotely on every action taken on the end-user's machine and can be remotely logged and has notable potential in industrial espionage as well as potential judicial repercussions (Simpson, 2003). This illustration demonstrates the potential of spyware to impact both commercial business and private citizens, irrespective of their locality. The reality is that spyware could be mining data (Thompson, 2005) on the end-user's machine, monitoring instant messaging (hereafter "IM") or monitoring voice conversations that utilize voice over internet protocol telephony (hereafter "VoIP") (Garrie, Harris, & Armstrong, 2005).

Web Enabled Installation of Spyware via Browser Vulnerability

The second type of spyware technology exploits vulnerabilities in web browsers or web-based applications to install themselves on end users' machines (Schultz, 2003). Functionally, the capabilities of the spyware installed are analogous to those installed via Shareware.

One main difference between the two types of spyware is that several studies suggest that Web-enabled spyware is declining (Moshchuk, 2005). It is difficult to determine the exact cause of the decline of this form of spyware, but it is likely due to several factors: (1) public awareness; (2) adoption of anti-spyware tools; and, (3) adoption of automated patch installation tools. These three elements have essentially helped prevent this type of spyware from capitalizing on technology based loopholes.

Adware is Different from Spyware

Spyware must be distinguished from adware. Adware, a modified derivative of cookie technology, places either random or targeted advertisements on the screen of the user (Wikapedia Spyware, 2005). Adware is generally not malicious because it does not collect and use personal information for illegitimate purposes (Wikapedia Spyware, 2005). Spyware, while similar to adware, is usually an application installed on the user's computer, and, by definition, is usually installed without the user's knowledge. Not only can spyware monitor users activities on the Web, but it can also monitor everything users do with their machines and transmit that information to an outside entity. Unfortunately, users mostly accept spyware unintentionally or without a full and informed understanding of its parameters when downloading something from the Web.

PRIVACY RIGHTS AND SPYWARE ON A GLOBAL STAGE

Spyware is a global problem; it is a problem in all six continents around the world. No particular country's laws have been able to slow the spread of spyware. In this section, we review European and U.S. law on the issue of data privacy, as applied to spyware. Data privacy rights vary from the U.S. to Europe, however, neither is particularly effective in protecting the public from the spyware epidemic.

Europe

Europe has established a much more stringent degree of personal data protection than the U.S. For instance, a U.S. company would be in violation of European human rights law by conducting electronic surveillance of European workers and transferring the results to countries like the U.S. that do not afford adequate privacy protection for employees' personally identifiable information (European Industrial Relations Observatory On-line, 2005). Today, the Constitution of Europe and various European Union directives, including Directive 2002/58/EC, form the framework of Europe's stringent digital privacy laws for individuals (European Commission, Privacy Protection, 2006).

Constitution of Europe

The Constitution of Europe is based on several successive treaties, most notably the Treaty of Rome (1957) and the Maastricht treaty (formally the Treaty on European Union, 1992), and has been modified by the more recent treaties of Amsterdam (1997) and Nice (2001). The Constitution was signed at a ceremony in Rome on October 29, 2004. Before it enters into force, however, it must be ratified by each state. This process was expected to take around two years to complete, but following the rejection in France and the Netherlands, the remaining process is now unclear. At the European Council of June 16-17, 2005, leaders extended the deadline beyond 2006, but did not set a new date.

The issue of privacy is addressed in Article 8 of the Constitution. Article 8 states that "[e]veryone has the right to respect for his private and family life, his home, and his correspondence" (European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950). The ECHR has extended the definition of "private life and correspondence" in Article 8 to encompass all business relations, e-mail, and associated electronic communications (See *Niemietz v. Germany* and *Halford v. United Kingdom*). Article 8 establishes a fundamental right to privacy that is granted to all individual citizens of E.U. countries under ECHR jurisdiction. Article 8 ensures protection of all communications irrespective of the means, which is distinct from U.S. law, where e-mail is given less protection than phone calls (Garrie, Harris, & Armstrong, 2005). This broad data privacy protection is triggered the instant information enters the boundaries of the E.U., irrespective of the medium used (Garrie, Harris, & Armstrong, 2005).

European Directives & Privacy

European Union Directives are collective decisions made by the member states, acting via their national Government Ministers, which participate in the Council of the European Union and the Parliament. A Directive requires that each member state implement legislation before it comes into effect in that state. Directives leave member states a significant amount of leeway as to the exact rules to be adopted. But if, the member state does not pass the requisite national legislation, or if the national legislation is inadequate respective to the requirements of the directive, the European Commission can initiate legal action against the member state in the European Court of Justice (hereafter "ECJ") (Mann, 2002).

Several European Directives have been passed over the years with respect to privacy. The first was in October 1995, when the EC adopted a directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data between member states (Directive 95/46/EC). Directive 95/46, which has been implemented by all the members States of the European Union, applies to all data, both paper and digital. Directive 95/46 defines the bounds between lawful and unlawful data processing to protect the rights and freedoms of persons who experience the processing of their own personal data. For instance, Directive 95/46 requires that any company collecting data on an individual must first obtain the consent of that individual and that the company must also identify itself to the people from whom it collects data, and allows those people to access the data so that they may make any necessary corrections.

Directive 95/46 was expanded by a new Directive on Privacy and Electronic communication in 2002, which targets specific privacy issues relating to electronic communications. The European Parliament passed the Directive 2002/58/EC on July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Directive 2002/58/EC, which has been adopted by the member states, applies to the collection, transmission, and processing of "personal data" within the EU. Processing of personal data is permitted if the data subject has unambiguously given his or her consent and in some other cases outlined in the text.

Directive 2002/58/EC requires a company seeking to gain access or to store information from a user's terminal (e.g., PC, mobile phone or other similar devices) to provide the user with clear information about the purpose of any such invisible activity and offer the user the right to refuse it (Directive 2002/58/EC). Directive 2002/58 further recognizes that the use of cookies presents multiple privacy and data protection problems even though they may serve a valid functional purpose in business (Garrie, Harris, & Armstrong, 2005).

Both Directive 2002/58 and Directive 95/46 bind not only service providers established in the territory of EU Member States, but also those established outside the EU, including the U.S. The Directives are ineffective in addressing the spyware wave for three reasons. First, the Directives lack a clear description of the exact interaction between Directive 2002/58 and its mother Directive 95/46. For instance, the Directive 2002/58 provisions apply to information processed via cookies that cannot be qualified as 'personal data' within the meaning of Directive 95/46. Second, neither Directive provides any concrete guidance as to how entities must comply with the obligations to provide information and to offer a right to refuse the installation of the spyware. For instance, a spyware application, by providing the user with the right to elect to install a shareware application, could arguably be offering the user the right to refuse the software. Third, it is not entirely clear what types of cookie uses are covered by the Directives. For instance, spyware applications that utilize technology that is a progeny of cookie-based technology, such as peer-to-peer web applications, are no longer obliged to comply with either of the Directives. Therefore, while the European Union directives provide a notably greater degree of protection of personal data privacy, they are generally ineffective in addressing the spyware wave.

United States' Law and Spyware

The law of the U.S. specifically addresses espionage, whether through the theft of government information or, as the law also contemplates, through stealing trade secrets or patentable information (*Rambus, Inc. v. Infineon*, 2004, p. 692). But what about the theft of other types of information from individuals' or business' computers? Most people are familiar with spyware's ability to infect computers and to record browsing habits, keystrokes, passwords, financial information, and other personally identifiable information and to transmit it without the computer owner's knowledge (Warkentin, 2005). Unfortunately for the person whose computer has been hijacked and whose information is being stolen, the law does not adequately address these types of spies, that is, spyware.

Today, the U.S. law has not developed to address spyware because spyware is a relatively recent phenomenon - a phenomenon that is really an extension of cookie technology. There are, however, three separate federal laws applicable in the spyware context: the Computer Fraud and Abuse Act (hereafter "CFAA") (2000 & Supp, 2004), The Stored Wire and Electronic Communications and Transactional Records Act (hereafter "Stored Communications Act") (2003); and the Wiretap Act (2000 & WestSupp., 2004). Unfortunately, none of these three acts were designed to address the issues presented by spyware, and each has significant drawbacks.

Under the CFAA (2000 & WestSupp., 2004), spyware victims can assert a civil cause of action provided they can show aggregate damages during a one-year period of at least $5,000.00, some modification or impairment of medical information, a physical injury, a threat to the public health or safety, or some damage to a government computer system. For the individual computer user, the only potentially applicable claim, and also the most difficult to establish, is the aggregate of $5,000.00 in damage. Even the most expensive personal computer costs much less than this (CFAA, 2000 & WestSupp., 2004). An alternative possibility would be for the individual to claim the loss of personal data exceeding the $5,000.00 limit (CFAA, 2000 & WestSupp., 2004). The question this raises for the individual consumer is whether litigation and the necessity of experts to show the extent of loss are worth the chance of recovery (CFAA, 2000 & WestSupp., 2004). For the individual consumer, without a class action, the potential value of the CFAA disappears. Furthermore, even if a class action arises, at least one of the members of the class must have $5,000.00 worth of damages to allow the other class members' claims to survive (CFAA, 2000 & WestSupp., 2004). The damage threshold eliminates the CFAA as an avenue of redress for most consumers. Under the Stored Communications Act (2000 & WestSupp., 2005) it could be argued that spyware violates the Act by collecting personal information from an individual through a communication without that individual's consent. The Act specifies a private cause of action to protect individuals in their privacy (Blakley, Garrie & Armstrong, 2005). The Stored Communications Act requires proof of five elements. The access must: (1) be to "a facility through which an electronic communication service is provided;" (2) be intentional; (3) exceed authorization; (4) "obtain, alter, or prevent" a wire or electronic communication; and (5) involve a communication maintained in electronic storage in that system (Stored Communication Act, 2000 & West Supp., 2005). This statute, in its current form,

does not provide US consumers with a remedy because of its broad construction of authorization. However, as with other potential remedies, if "authorization" can be redefined, a remedy may exist.

The Wiretap Act (2004) would seem to be the best avenue to address spyware. However, unlike the Stored Communications Act, courts have limited its provisions to apply only to the interception of electronic information in transit, (Wiretap Act, 2000 & West Supp. 2004) The Wiretap Act was designed not only to protect digital communications, but to protect telephone calls over traditional networks (Garrie, Harris, & Armstrong, 2005). Spyware companies have taken advantage of the storage-transit dichotomy to develop programs that intercept communications while they are in a temporarily stored state, either prior to, or immediately after transmission (Garrie, Harris, & Armstrong, 2005). While providing some legal viable recourse for the user, the Wiretap Act does not provide a comprehensive civil or criminal remedy.

Adjoining these aforesaid legal remedies are two traditional tort theories that may be effective in attempting to address spyware: trespass to chattels (Restatement (Second) of Torts § 218, 1965); and intrusion upon seclusion (Restatement (Second) of Torts § 652B, 1977). Neither common law theory has proven particularly successful (Blakley, Garrie & Armstrong, 2005). First, the tort of trespass to chattels is marginally helpful because of the difficulty in establishing damage to the chattel and the argument of implied consent. Second, the tort of intrusion upon seclusion focuses on consent and depends upon whether a court finds that a victim's expectation of privacy is reasonable or that the spyware perpetrator has a duty to prevent harm to the victim (Restatement (Second) of Torts § 652B, 1977).

This type of weakness in the extant law demonstrates why the judiciary's role is extremely important regarding spyware cases. Irrespective of a court's point of view in imposing or denying liability, the current common law fails to meet the needs of the consumer or of businesses in addressing spyware. Courts must be creative in applying the law to these new situations.

SPYWARE SOLUTIONS

While all of the potential remedies described above may provide assistance for some consumers and businesses in certain countries under the right circumstances, most spyware has been able to bypass any criminal or civil liability. Country-specific statutory solutions will probably be ineffective to impede the propagation of spyware and other data mining technologies. Rather the only viable solution is for countries to join together to implement uniform digital privacy protection laws that significantly improve international digital privacy law remedies.

Multi-click Consent Agreements

One potential statutory improvement that would help minimize unknowing consent by the user, and consequently eliminate most spyware, is by requiring general acceptance of EULA terms, as well as specific acceptance at all relevant points where access is granted to the user's personal information. The multi-click consent agreement itself should use language that can be understood by a layperson.

This multi-click consent solution would have three benefits. First, users will be better protected against "piggyback" spyware applications, because multi-click consent ensures that users are no longer unknowingly consenting to the installation and operation of spyware applications through a cumbersome, incomprehensible and, generally unread, EULA (Eunjung, 2004). For instance, "piggyback" spyware applications, such as Kaza, would no longer be able to embed in their EULA a provision granting consent to the installation of spyware applications that are invisible to the user. Instead, the multi-click EULA would bring to the user's attention a specific consent component that would only grant the spyware permission to install and operate on the user's machine *after* the user is informed in plain and unambiguous language of the personal data that the spyware may be record. Therefore, "piggyback spyware" that operates via the EULA loophole would be greatly limited because they would not be able to obtain the user's consent to the software installation via a cumbersome EULA. Instead the consumer would be informed and educated about the "piggyback spyware" being installed on their machine.

Second, the multi-click consent solution would benefit companies that utilize spyware applications for valid commercial purposes. The explicit multi-click consent EULA would provide evidence to rebut claims by users that the companies' spyware operated in a manner "invisible" to the user. For instance, a company could rebut a user's claim that the company obtained personal information without the user's consent with real-evidence of the user's explicit multi-tiered consent to the installation and operation of the software.

Third, the multi-click consent solution would enable the law to differentiate between data mining of the type done by companies that monitor which pages visitors view on their own websites (a practice with clear commercial advantages that does not violate the end user's personal privacy) from the type of data mining done by spyware programs that are actually installed on the end user's personal computer and monitor key-strokes, passwords, and the like (Bono, 2005) without the user's consent.[2] The construction of this distinction will facilitate civil and/or criminal prosecution of unlawful spyware because such spyware would lack the user's consent, whereas lawful spyware would have the user's consent. Thus, the multi-tiered consent solution indirectly addresses unlawful spyware while directly addressing the highly problematic "piggyback spyware" issue. Most importantly, the average user will be protected from the misleading and cumbersome consent agreements through which "piggyback spyware" currently operates.

In order to effectively implement a multi-click consent EULA, a uniform consent clause should be developed to standardize the statement of intent to mine personal data. All nations should be encouraged to adopt uniform legislation to prevent spyware companies from capitalizing on different countries' laws. This uniform statement would inform users of the potential risks associated with granting consent to the installation and operation of a spyware application on their machine. The statement would be analogous to the health warnings found on cigarette cases in most developed countries that inform consumers of the health risks of smoking (World Health Organization, 1999).

While the data mining and spyware industries are likely to resist to any such multi-click consent requirement, spyware is analogous to cigarettes in that consumers should at the very least be informed of the potential harm that they may incur. Even though cigarette manufacturers resisted warnings, many countries require them for the physical health of their citizens (Mahood, 1995). Similarly, countries should require multi-click consent requirements for the "privacy health" of their citizens.

This special consent language should be inserted into the EULA and brought to the user's attention, requiring that the user give explicit multi-click consent. Like cigarette smokers, end users would still be able to allow spyware to operate on their systems if they choose to do so. The only difference would be that the end users would be able to make an informed choice just as those who smoke do so knowing full well of the harms that prolonged exposure to noxious cigarette fumes can cause to their bodies. Utilizing this multi-click consent approach incorporating explicit consent language would greatly alleviate unwanted privacy intrusions by data mining programs by refining consent agreements to preclude click-through consenting (Blakley, Garrie & Armstrong, 2005). This can be developed further by perhaps adding a "civil enforcement" provision that gives significant civil damages to aggrieved individuals irrespective of their actual losses to help ensure that perpetrators who mine personal data without informed consent are brought to justice.

Potential Non-Statutory Solutions

While the international community is increasingly regulating activities on the Internet with promising statutory laws (Rundle, 2005), another viable tool for preventing spyware privacy infringements is to give courts access to information about emerging technologies and their potential to violate individuals' rights. It is imperative that courts around the world be empowered to apply existing privacy laws in their respective countries to new cases involving data processing disputes. This is especially true because many countries have adopted legislation, such as the European Directive of 1995, which could be applied to spyware. Judges need to have access to enough available information to fully understand the technologies and how they are being used, or could be used, to violate the law (Nesson, 2005).

Such a curriculum might include a combination of on-line, in-person, and paper materials, and could utilize a variety of educational tools, so as to maximize accessibility to all judges across national borders. By standardizing not only data mining law, but also the technical education and methods of applying such laws to specific cases, those who use spyware technologies for unethical ends will be at a tremendous disadvantage. Judicial education would help to establish a complete and potentially consistent body of case law in the international community as judges would have full understanding of how much privacy infringement data mining technologies are capable of. Ideally, an internationally standardized technology curriculum for judges could be an extremely useful aid to justices presiding over privacy disputes involving new technologies.

CONCLUSIONS

Notwithstanding their fundamentally different perspectives on digital privacy, changes to the legal infrastructure in the U.S or the E.U. will provide a great starting point to address the global problem of spyware. Implementing such changes would provide a cooperative model for the rest of the world. It is important that the legal reform expand beyond both the U.S. and the E.U. because spyware and other technological problems are not geographically bound. For instance, most software piracy is not U.S. or E.U. based. Furthermore, as new technologies emerge beyond the confines of cookie technology or even Internet based spyware, countries around the world will find themselves confronting the challenge of protecting their citizens' personal information. Spyware has no borders and is not confined to any particular U.S. state or E.U. member.

Accordingly, spyware must be addressed at a global, not country-specific, level. Perhaps the U.N. and International Court of Justice can contribute toward the creation of a global information privacy framework. Even though such a solution could not apply to a governmental actor, it would impact those who operate spyware technologies for personal or private purposes.

Irrespective of whether a country-specific or global approach is taken, those tasked with applying these statutes and laws should receive training and education on spyware and all emerging technologies. By educating those tasked with interpreting the laws, fewer judicial loopholes will be created. For instance, if the legislature and judiciary were better educated about how the Internet operates as whole, the development of laws regarding spyware and other internet data mining technologies would inevitably afford individuals greater protection and peace of mind.

REFERENCES

Adelman, B., (2005). *Gator's EULA Gone Bad* retrieved July 13, 2005 from the World Wide Web: http:// www.benedelman.org/news/112904-1.html

Blakley, A., Garrie, D. B., & Armstrong, M.J., (2005). Coddling spies: why the law doesn't adequately address computer spyware. *Duke Law & Technology Review 2005*. Retrieved February 6, 2006 from http://www.law.duke.edu/journals/dltr/articles/2005dltr0025.html

Bono, M., (2005). Are you aware of spyware on your home computer? *The Hill.* Retrieved March 7, 2006 from the World Wide Web: http://www.hillnews.com/thehill/export/TheHill/News/Frontpage/102005/ssbono.html

Brandt, A., (2000). How it Works: Cookies. *PcWorld.* Retrieved Aug. 10, 2004 from the World Wide Web: http://www.pcworld.com/hereshow/article/0,aid, 15352, 00.asp

Byers, S. (2001). The Internet: Privacy Lost, Identities Stolen, Brandeis Law Journal, 141, 143-44.

Carfarchio, P. (2002). The challenge of non-viral malware, PestPatrol White Papers. Retrieved Aug. 2, 2002 from World Wide Web: http://www.pestpatrol.com/Whitepapers/NonViralMalware0902.asp

Computer Fraud and Abuse Act 18 U.S.C. §1030 (2000 & WestSupp. 2004). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23 November 1995.

Directive 2002/58/EC, (12 July 2002). Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), O.J. L 201/37, 31 July 2002, replacing Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector, O.J. L 53, 14 January 1998.

Eunjung Cha, A. (2004). Computer users face new scourge; hidden adware programs hijack hard drives. The *Washington Post*, A01.

European Commission Privacy Protection (2005). *Privacy Protection.* Retrieved March 3, 2006 from the World Wide Web: http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm (last updated Mar 6, 2006)

European Convention for the Protection of human rights and fundamental freedoms (1950). Council of Europe, Rome, , http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm; See also article 7 of the Charter of Fundamental Rights of the European Union, O.J. C 364/1, 18.12.2000.

European Industrial Relations Observatory On-line (2005). *New Technology and Respect for Privacy at the Workplace 5*. Retrieved March 1, 2006 from the World Wide Web: http:// www.eiro.eurofound.eu.int/print/2003/07/study/tn0307101s.html

Foster, E. (2002). The gripe line: the spy who loves you - some 'free' internet services come with the kind of surveillance you may not want. *Infoworld,* 60(60), 24.

Garrie, D. B., Armstrong, M., & Blakely A., (2005). Voice over internet protocol: reality v. legal fiction. *Federal Lawyer,* 7, 34 - 36.

Garrie, D., Armstrong, M. & Harris, D., (2005). Is Your Conversation Protected?, *University of Seattle Law Review,* 27, 97 – 113.

Gibson, S. (2005). OptOut retrieved May 10, 2005 from the World Wide Web: http://www.grc.com/oo/news.htm.

Gordan, S. (2005). Fighting spyware and adware in the enterprise. *Information Systems Security ISC2 Journal,* 14. Retrieved March 8, 2006 from http://www.infosectoday.com/

Halford v. United Kingdom, 39 Eur. Ct. H.R. 1004 (1997).

Hagerty, J. R. & Berman, D.K. (2003, August 27). Caught in the net: new battleground over web privacy: ads that snoop. *Wall Street Journal,* A1.

Hamilton, J. (1972). The demand for cigarettes; advertising, the health scare, and the cigarette advertising ban. *Review of Economics and Statistics*, 54(4), 401-411.

Kenkel, D. S. (1991). Health behavior, health knowledge, and schooling. *Journal of Political Economy*, 99(2), 287-305.

Klang, M. (2004). Spyware - the ethics of covert software. *Ethics and Information Technology*, 193-202.

Krause, J. (2005). Prying Eyes, 91(5) *A.B.A.J.* 60 May 2005, Vol.91 Issue 5, p. 60, 2p, 1c.

Lavasoft, Spyware & Harmful Technologies. Retrieved Sept. 19, 2005 from the World Wide Web: http://www.lavasoftusa.com/trackware_info/spyware_tech

Lippert, S. K. & Swiercz, P. M. (2007). Personal Data Collection via the Internet: The Role of Privacy Sensitivity and Technology Trust, *Journal of International Technology and Information Management* ,Vol.16, Issue 1, 17-30.

Levy, S. & Stone, B. (2005). Grand theft identity. *Newsweek,* p. 38.

Mann, R. & Winn, J., (2002). *Electronic Commerce* 187 (stating that data protection varies notably across member states: Germany, France, and United Kingdom had a tradition of strong protection of privacy versus non-existent regulation in Greece.)

Moore, D. (2003). Inside the slammer worm. *IEEE Security & Privacy*, 33-39.

Nesson, C. R. (2001). Online privacy. Retrieved January 24, 2006, from http://cyber.law.harvard.edu/ilaw/Privacy

Nesson, C., Marino, A., & Kent, R. (2005). Privacy. Retrieved January 24, 2006, from http://cyber.law.harvard.edu/ilaw/harvard_2005_module_3_privacy

Mahood G. (1995). Canadian tobacco package warning system. Tobacco Control, 4, 10–14.

Moshchuk, A., Bragin,T., Gribble, S., & Levy, H., A (2006). Crawler-based Study of Spyware on the Web Department of Computer Science & Engineering University of Washington. Retrieved March 2, 2006 from the World Wide Web: http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf

Niemietz v. Germany, 251 Eur. Ct. H.R. 23 (1992).

Prostic,E. (2004). Remarks, Monitoring Software on Your PC: Spyware, Adware, and Other Software (Spyware Workshop, April 19, 2004), Retrieved July 20, 2004, from

http://www.ftc.gov/bcp/workshops/Spyware/index.htm

Rambus, Inc. v. Infineon Tech. AG, 330 F. Supp. 2d 679, 692-93 (E.D. Va. 2004).

Restatement (Second) of Torts § 652B, (1977).

Restatement (Second) of Torts § 218, (1965).

Rundle, M. C. (2005). Beyond internet governance: the emerging international framework for governing the networked world. Retrieved January 24, 2006, from http://cyber.law.harvard.edu/home/2005-16

Ryker, Randy M. & Bhutta, Khurrum S. (2005). Online Privacy Policies: As Assessment of the Fortune Global 100, *Journal of International Technology and Information Management* ,Vol. 14, Issue 1, 15-24.

Schor, E (2005). Pornography: Not your typical Senate hearing. The Hill. Retrieved March 7, 2006 from the World Wide Web: http://thehill.com/thehill/export/TheHill/Features/CapitalLiving/012506_porn.html

Schultz, E. (2003). Pandora's box: spyware, adware, autoexecution, and NGSCB. *Computers & Security*, 22(5), 366.

Spiror, J. C., Ward, B. T., & Roselli, G.R. (2005). The ethical and legal concerns of spyware. *Journal of Information Systems Management*, 22(2), 39-50.

Stored Wire and Electronic Communications and Transactional Records Act 18 U.S.C. § § 2701-11 (2000 & West Supp. 2005).

Thompson, R. (2003). Cybersecurity & consumer data: what's at risk for the consumer? Retrieved Dec. 27, 2005, from The Information Warfare Site Web site: http://www.iwar.org.uk/comsec/resources/consumerrisk/Thompson1799.html

Urbach, R., & Kibel, G. (2004). Adware/spyware: an update regarding pending litigation and legislation. *Intellectual Property & Technology Law Journal*, 7, 12-16.

U.S. Dep't of Commerce News (2000). *U.S Census Bureau, Retail E-commerce Sales for the Fourth Quarter 1999 Reach $5.3 Billion* retrieved March 30, 2005 from the World Wide Web: http://www.census.gov/mrts/www/current.html

Volkmer, C. J. (2004). Will adware and spyware prompt congressional action? (or does my computer's cd tray open for no apparent reason?). *Internet Law*, 11(7), 1.

Warkentin, M., Luo X, & Templeton G.F. (2005). A Framework for Spyware Assessment, *Communications of the ACM*, 48, p. 8.

Weir, E. (2005). A European perspective on offshoring and data protection. *Practical Lawyer*, 51, 3, 49-53.

Webopedia (2005). Spyware. Retrieved Sept. 19, 2005 from the World Wide Web: http://www.webopedia.com/DidYouKnow/internet/2004/spyware.asp

Wildstrom, S. (2004). How to stymie the snoop in your pc. *Business Week*, 28.

Wilson, J. (n.d.). How Toptext works. Retrieved December 27, 2005, from Scumware.com Web site: http://scumware.com/wm2.htm

Wiretap Act 18 U.S.C §2510 et seq. (2000 & Supp. 2004).

World Health Organization (1999). *World Health Report 1999: Making a difference. Chapter 5: Combating the tobacco epidemic. Geneva: WHO.* Retrieved March 3, 2006, from http://www.who.org/tob/.

[1] An end-user can view all of the cookies stored on a local machine using Internet Explorer by following these steps: (1) open Internet Explorer; (2) select "Internet Options" under the "Tools" menu; (3) click on the "General" tab and click the "Settings" button; (4) click the view files button; (5) sort files by type by clicking on "Type"; (6) find documents of the type labeled "Text Document." To see the information stored by the cookie in its raw and likely unintelligible format, double-click on one of these text files containing, "cookie" in its file name.

[2] It is beyond the scope of this paper to provide the technical details of how such technology would operate, but further information is available from Daniel Garrie.