SCRIPT-ed

Volume 3, Issue 3, June 2006

Parasiteware: Unlocking Personal Privacy

Daniel B. Garrie[*] *& Rebecca Wong*[+]

Abstract

Spyware presents a threat of privacy infringement to unassuming internet users irrespective of their country of citizenship. European legislation attempts to protect end-users from unethical processing of their personal data. Spyware technologies, however, skirts these laws and often break them in their entirety. Outlawing the spyware and strengthening the legal consent requirement to mine data are statutory solutions that can prevent spyware users from skirting the law. An internationally standardized technology education system for the judiciaries in Europe and the U.S. can help ensure that when spyware users do break the law, they cannot hide by escaping from one nation to another without being held accountable. Transnational improvements are necessary to remedy the global spyware epidemic.

DOI: 10.2966/scrip.030306.203

[*] Daniel B. Garrie is the CEO of Lexeprint, Inc, a firm specializing in providing Global Justice Solutions and innovative printing technologies. Mr. Garrie has received his J.D. from Rutgers University School of Law, and has penned several law review articles on a variety of technology and legal issues. Mr. Garrie holds an M.A. and B.A. in computer science from Brandeis University. Mr. Garrie has worked around the world with the various Government agencies and corporations as a Senior Consultant. Mr. Garrie currently resides in New York City. Mr. Garrie can be reached at Daniel.Garrie@gmail.com.

[+] Rebecca Wong is a Lecturer in Law at the School of Law, Nottingham Law School. Her main areas of specialism are in data protection and privacy. She holds an LLB (1998), MSc (2000), LLM (2001) and has recently completed her PhD in data protection.

1. Introduction

With today's rapid rate of technological advancement, it is imperative that judicial systems around the world evolve their legal systems to address the spyware problem. Digital privacy is not limited to a specific geographical boundary. As societies become more dependent on technology, the need for greater awareness, action and education to help protect average citizens from all misuses of technology can alleviate this dilemma.

Although Europe has implemented quite strict data processing protection laws, far beyond those within the U.S,[1] little has been achieved to protect European Internet users from spyware.[2] Left largely unchecked by legal remedies, spyware has infiltrated and overrun personal computers worldwide. This paper elucidates the threat of spyware in the light of its technical capabilities, analyzes how spyware violates existing European law, and provides solutions, statutory and non-statutory. [3]

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.[4] An AOL/National Cyber Security Alliance (NCSA) Online Safety Study further supports this, recently reporting that 80 percent of scanned computers contain a derivation of spyware or adware.[5] Irrespective of the precise number of infected machines it is clear that spyware exists and is growing in our computer-driven society.

2. 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.[6] Most users find cookies beneficial because they "[e]liminate the need to repeatedly fill out order forms or re-register on Web sites."[7] For instance, with passwords being increasingly

[1] See J. Reidenberg, & P. Schwartz, *Data privacy law* (Michie, Charlottesville, Va 1996); P. Swire and R.E. Litan, *None of your business*: *world data flows, electronic commerce, and the European privacy directive* (Brookings Institution Press, Washington DC 1998) and E Weir. A European perspective on offshoring and data protection, 2005 *Practical Lawyer*, 51, 3, 49-53.

[2] S. Levy. & B. Stone. 'Grand theft identity' (2005) *Newsweek* 38 @ <http://www.msnbc.msn.com/id/9108639/site/newsweek> accessed March 8 2006

[3] For a description of losses due to identity theft and the potential liability of those stealing the information, see S. Byers. 'The Internet: Privacy Lost, Identities Stolen' (2001) *Brandeis Law Journal*, 141, 143-44.

[4] S. Gordan. 'Fighting spyware and adware in the enterprise' (2005) *Information Systems Security ISC2 Journal* 14. @ <http://www.infosectoday.com/> accessed March 8, 2006.

[5] Ibid.

[6] Ibid.

[7] Ibid.

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 examples of modifications of legitimate cookie technology are such tools as 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 all examples of modifications of cookie technology.[8]

2.1. 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.[9] Spyware is the progeny of clickstream data or cookie based data mining technology.[10] 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. 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[11] 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.[12] In the world of technology, "Spyware" is the umbrella term under which numerous technologies, both legal and malicious fall, including: adware[13]; trojans; hijackers;[14] key loggers;[15] malware;[16] and, dialers.[17]

[8] Lavasoft. 'Spyware & Harmful Technologies' @ <http://www.lavasoftusa.com/trackware_info/spyware_tech> accessed Sept. 19, 2005

[9] S. Gordan, see note 6.

[10] A. Brandt, A., How it Works: Cookies. *PC World.* @ <http://www.pcworld.com/hereshow/article/0,aid,15352,00.asp> accessed August 10, 2004.

[11] 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' @ <http://www.census.gov/mrts/www/current.html> accessed March 30, 2005.

[12] B. Adelman, 'Gator's EULA Gone Bad' @ <http://www.benedelman.org/news/112904-1.html> accessed July 13, 2005.

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

[14] J. Wilson. (n.d.), 'How Toptext works' @ <http://scumware.com/wm2.htm> accessed December 27, 2005.

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

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.[18] 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. [19]

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.[20] 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.[21] 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[22] it is able to access the end-user's electronic file system,[23] e-mail system, web pages viewed, and any other information the end-user accesses on the machine that is not encrypted.[24]

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,[25] unbeknownst to the end-user,[26] 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.[27] As Krause[28] points out generally, malicious spyware tends to be financially motivated, distinguishing itself from past viruses/malware.

[16] P. Carfarchio, 'The challenge of non-viral malware' *PestPatrol White Papers*. @ <http://www.pestpatrol.com/Whitepapers/NonViralMalware0902.asp> accessed Aug. 2, 2002.

[17] J. Wilson, see note 16.

[18] J.C. Spiror,, B.T. Ward, & G.R. Roselli. 'The ethical and legal concerns of spyware' (2005) *Journal of Information Systems Management*, 22(2), 39-50.

[19] J. Wilson, see note 16.

[20] Ibid.

[21] E. Schultz, see note 17.

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

[23] E. Prostic, 'Remarks, Monitoring Software on Your PC: Spyware, Adware, and Other Software' (Spyware Workshop, April 19, 2004) @ <http://www.ftc.gov/bcp/workshops/Spyware/index.htm> accessed July 20, 2004.

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

[25] S. Gibson. 'OptOut' @ <http://www.grc.com/oo/news.htm> accessed May 10, 2005.

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

[27] J. Krause, 'Prying Eyes' May 2005, 91(5) *A.B.A.J.* 60.

2.2. 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.

2.2.1. Software Enabled Installation of Spyware via Shareware

As Moshchuk, Bragin, Gribble and Levy,[29] researchers from University of Washington Department 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.[30] 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.[31] Software-enabled spyware that relies on this attachment mechanism for installation has been coined "piggy-backed spyware."[32]

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,[33] 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.[34] For instance, spyware is frequently used in e-cards, via a commercial trojan spyware be it romantic, joke and others with which to ensnare your victim.[35] 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.[36] 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.[37] This illustration demonstrates the potential of spyware to impact both commercial business and private citizens, irrespective of their

[28] Ibid.

[29] T. Moshchuk (et. al). 'A Crawler-based Study of Spyware on the Web' *Department of Computer Science & Engineering University of Washington* @ <http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf> accessed March 2, 2006.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] N. Leibowitz, M. Ripeanu, and A. Wierzbicki. 'Deconstructing the Kazaa Network' *Proc. of The Third IEEE Workshop on Internet Applications,* June 23-24 2003. San Jose, CA, 2003, 112.

[34] Ibid.

[35] A. Blakley, D.B. Garrie, & M.J. Armstrong, Coddling spies: why the law doesn't adequately address computer spyware. *Duke Law & Technology Review* (2005) 25. @ <http://www.law.duke.edu/journals/dltr/articles/2005dltr0025.html> accessed February 6, 2006.

[36] K. Poulson. 'E-card sneakware delivers web porn' @ <http://www.securityfocus.com/news/1350> accessed Aug 8, 2006.

[37] Ibid.

locality. The reality is that spyware could be mining data[38] on the end-user's machine, monitoring instant messaging [hereafter "IM"] or monitoring voice conversations that utilize voice over internet protocol telephony [hereafter "VoIP"].[39]

2.2.2. 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.[40] 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.[41] 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.

2.2.3 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.[42] Adware is generally not malicious because it does not collect and use personal information for illegitimate purposes.[43] 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.

2.3.4. Parasiteware Emerging Privacy Evading Technology

To date the digital world has seen a wide range of privacy evading technologies, but a new set of technologies are cropping up that do more than just spy on the user and can

[38] R. Thompson. 'Cybersecurity and consumer data: what's at risk for the consumer?' @ <http://www.iwar.org.uk/comsec/resources/consumerrisk/Thompson1799.htm> accessed Dec. 27, 2005.

[39] D.B. Garrie, M.J. Armstrong, D. Harris, 'Is Your Conversation Protected?' *University of Seattle Law Review*, 27, 97 – 113 (2005).

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

[41] A Moshchuk, (et. al.) 'A Crawler-based Study of Spyware on the Web' *Department of Computer Science & Engineering University of Washington.* Retrieved March 2, 2006 @ http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf.

[42] Webopedia, 'Spyware' @ <http://www.webopedia.com/DidYouKnow/internet/2004/spyware.asp> accessed Sept. 19, 2005

[43] Ibid.

be termed "parasitewares".[44] Why parasiteware?[45] These new technologies are parasitic in nature because they are accompanying e-mail messages, software programs, or cell phone applications and the user is unaware that the application is installing itself. This suite of technologies can be used to spy, monitor, or steal the end-user's digital information.

3. 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.[46] In this section, we review European and U.S. law on the issue of data privacy, as applied to spyware. This section also takes into account the Framework Decision on attacks against information systems that was passed on 24 February 2005. Although data privacy rights vary from the U.S. to Europe, neither is particularly effective in protecting the public from the spyware epidemic.

3.1. 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

[44] While not defined as such the concept is derived from a survey of technological information sources. See S. B. Spencer, 'Reasonable Expectations and the Erosion of Privacy' 39 *San Diego L. Rev*. 843, 910 (2002); see K. Walker, 'The Costs of Privacy' 25 *Harv. J.L. & Pub. Policy* 87, 113-117 (2001); D. J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' 53 Stan. L. Rev. 1393, 1458-60 (2001); L. Jenab, Comment, 'Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress' 49 Kan. L. Rev. 641, 667-68 (2001); R. K. Zimmerman, 'Note, The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century' 4 N.Y.U. J. Legis. & Pub. Policy 439, 459-60 (2000).; A. Z. Naider, 'Distinguishing Software-Based Contextual Marketing Technology from Spyware, U.S. Senate Committee on Commerce, Science and Transportation' (2004), available @ <http://commerce.senate.gov/pdf/naider032304.pdf>; M. Klang, Spyware: 'Paying for Software With our Privacy' 17 *Intl. Rev. L. Computers & Tech* 313 (2003); A. Moshchuk (et. al.) 'Crawler-based Study of Spyware on the Web' Department of Computer Science & Engineering University of Washington, www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf. (accessed Mar. 2, 2006); KaZaA 'Hack 3.0', at http://www.kazaahack.net/home.html (last visited Nov. 17, 2005).; E. Foster, 'The Gripe Line: The Spy Who Loves You-Some 'Free' Internet Services Come With the Kind of Surveillance You May Note Want' 24 *Infoworld* 60, 60 (May 20, 2002).; D. Radcliff, 'Spyware' 4(21) Network World 51 (2004); Roger Thompson, 'Cybersecurity & Consumer Data: What's at Risk for the Consumer?' Testimony before the U.S. House of Representatives Subcommittee on Commerce, Trade, and Consumer Protection, http://www.iwar.org.uk/comsec/resources/consumerrisk/Thompson1799.htm. (accessed Dec. 27, 2005); TUT (International Telecommunications Union) Recommendation H.225.0, Call Signaling Protocols and Media Stream Packetization for packet Based Multimedia Communication Systems (1998).

[45] Ibid.

[46] See CERT Coordination Center, CERT/CC Statistics 1988-2005, http://www.cert.org/stats#incidents (last visited Apr. 9, 2006) (documenting that the problems of such technology are only growing).

employees' personally identifiable information.[47] Today, the European Union Directives, including the Directive on Privacy and Electronic Communications 2002/58/EC form the framework of Europe's stringent digital privacy laws for individuals.[48]

3.1.1. The European Union

The European Union 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 Treaties of Amsterdam (1997) and Nice (2001).[49] Recently, the Constitutional Treaty (hereinafter "CT") 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.[50] 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 European Convention of Human Rights 1950 (hereinafter "ECHR"). Article 8 states that "[e]veryone has the right to respect for his private and family life, his home, and his correspondence." 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*[51] and *Halford v. United Kingdom*[52]). Article 8 establishes a fundamental right to privacy that is granted to all individual citizens of European Union 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.[53] Art. 8 EHCR, however, is not absolute and can be derogated under Art. 8(2) where this was in accordance with the law and was necessary in a democratic society.[54] The main exceptions to Art. 8(2) are national security; public safety or the economic well-being of the country; for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. This broad data privacy protection is triggered the

[47] Art. 25 of the Data Protection Directive 95/46/EC. See also European Industrial Relations Observatory On-line (2005) 'New Technology and Respect for Privacy at the Workplace' 5 @ <http://www.eiro.eurofound.eu.int/2003/07/study/tn0307101s.html> accessed March 1, 2006.

[48] European Commission, *Data Protection* @ <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm> accessed Sep 6, 2006).

[49] K. Lenaerts, & P. Van Nuffel, *Constitutional Law of the European Union,* (2nd ed. Sweet & Maxwell, London 2005) at 67-75.

[50] N. Foster (ed). *Blackstone's Statutes: EC Legislation 2005/2006* (16th ed. OUP, Oxford 2005) at xxvii-clxii.

[51] (1993) 16 EHRR 97.

[52] (1997) 24 EHRR 524.

[53] D.B Garrie, M.J. Armstrong, D. Harris, "Is Your Conversation Protected?" *University of Seattle Law Review*, (2005) 27, 97 – 113.

[54] See e.g. *Handyside v United Kingdom* (1979) 1 EHRR 737 and *Sunday Times v United Kingdom,* (1970-80) 2 EHRR 245. The European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol 11, Nov. 4, 1950 can be found at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm, (last visited Sept. 4, 2006).

instant information enters the boundaries of the E.U., irrespective of the medium used.[55]

3.1.2. The Data Protection Framework in Europe

European Union Directives (Art. 249 EC) 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"] [56]).

There are two main Directives that address the issue of 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 (hereinafter "Data Protection Directive 95/46/EC"). The Data Protection Directive 95/46, which has been implemented by all the member states of the European Union, applies to all data, both paper and digital. The Data Protection Directive 95/46 defines the boundaries between lawful and unlawful data processing to protect the rights and freedoms of persons who experience the processing of their own personal data (Art. 1(1) Data Protection Directive). For instance, the Directive 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.

The Data Protection Directive 95/46 was expanded by a new Directive on Privacy and Electronic Communications in 2002 (hereafter "Directive 2002/58/EC), which targets specific privacy issues relating to electronic communications (Art. 1(1) Directive 2002/58/EC). 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. Art. 2(2) expressly provides that the provisions of Directive 2002/58/EC particularise and complement Directive 95/46/EC. Directive 2002/58/EC has been adopted by the member states and 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. (Art. 5(3) Directive 2002/58/EC). Directive 2002/58 further recognizes that the use of

[55] Ibid.

[56] See Art. 226 of the EC Treaty, which enables the European Commission to instigate legal action against a member state for failing to fulfil its obligations under EC Law.

cookies presents multiple privacy and data protection problems even though they may serve a valid functional purpose in business.[57]

Both Directive 2002/58/EC and the Data Protection Directive 95/46/EC bind not only service providers established in the territory of EU Member States, but also those established outside the EU, including the U.S (Art. 4(1)(c) of the Data Protection Directive 95/46/EC). The Directives are ineffective in addressing the spyware wave for three reasons. Firstly, the Directives lack a clear description of the exact interaction between Directive 2002/58 and its mother the Data Protection Directive 95/46.[58] 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. Secondly, 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. Furthermore, knowledge of spyware cannot be equated with the user's consent to spyware. The original proposals for an opt-in consent under the Directive 2002/58/EC were watered down.[59] Directive 2002/58/EC does not exactly define the scope of "spyware". Recital 24 of the Directive 2002/58/EC provides that 'so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users.' In the absence of a definition, a purposive interpretation should be adopted. In other words, do such devices have the effect of tracing the activities of the user (with or without their knowledge)? It should also be added that the use of such devices are permitted for legitimate purposes and with the knowledge of the users. However, what is unclear is how spyware or for that matter, any devices that are traceable to the user can be allowed for a legitimate purpose? Referring to recital 25 of the Directive 2002/58/EC, the use of cookies to facilitate the provision of information society services is considered to be a legitimate purpose, but it is questionable whether spyware can fall within the same category as cookies. Thirdly, it is not entirely clear what types of cookies the Directives covers. 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.

[57] D.B. Garrie, M. Armstrong, & D. Harris, see note 55 and Recitals 24 and 25 of Directive on Privacy and Electronic Communications 2002/58/EC.

[58] Recital 10 of Directive 2002/58/EC provides that 'Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive [2002/58/EC], including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to *non-public communications services*' (emphasis added). See also the Art. 29 Working Party. 'Privacy on the internet – an integrated EU approach to online data protection' @ <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf> accessed May 23, 2006.

[59] See Common Position 26/2002 of 28 January 2002 adopted by the Council, acting in accordance with the procedure referred to in Art. 251 of the Treaty establishing the European Community, with a view to adopting a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector *EU Official Journal* 14 May 2002, C 113/39.

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.

3.1.3 Framework Decision 2005/222/JHA on Attacks against Information Systems

The Framework Decision[60] was passed on 24 February 2005 and aimed to 'improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States [of the European Union] in the area of attacks against information systems.' (Recital 1 of the Framework Decision).

The purpose of this section is not to describe the Framework Decision in its entirety but provide a critique of the relevant provisions that relate to spyware and consider its limitations.

To begin with, framework decisions were introduced under the 1997 Amsterdam Treaty.[61] They are binding upon the Member States as to the result to be achieved but national authorities determine how this would be implemented (Art. 34 of the Consolidated Version of the Treaty on European Union uses the words 'the choice of form and methods to achieve the result').

The main objective of the Framework Decision was to harmonise the laws or any offence committed against a computer infrastructure with the intention of destroying, modifying or altering the information stored on computers or networks of computers.[62] The Framework Decision addresses the issues of hacking, computer viruses; denial of service attacks and so forth (Arts. 2-4 Framework Decision). The Framework Decision differentiates between illegal access to information systems under Art. 2; illegal system interference under Art. 3; and illegal data interference under Art. 4. Art. 3 is relevant in the context of spyware, because it enumerates the categories in which an illegal system interference may occur. In particular, Art. 3 covers 'intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data.' Commission of these three offences are punishable as a criminal offence and the perpetrator(s) should have committed these offences *intentionally* (Arts. 2, 3, and 4 uses the words "cases which are not minor"). The Framework Decision does not appear to criminalise *minor* offences. Art. 6 states that 'each Member State shall take the necessary measures to ensure that the offences referred in Articles 2, 3, 4 and 5 are punishable by *effective*, *proportional* and *dissuasive* criminal penalties.' Art. 5 covers the areas of instigation, aiding, abetting and attempt. Art. 6 further provides that these criminal penalties

[60] OJ L069, 16.3.2005, at 67-71.

[61] Art. 34(2b) of the Consolidated Treaty on European Union confers powers on the European Council to 'adopt framework decisions for the purpose of approximation of the laws and regulations of the Member States. Framework decisions shall be binding upon the Member State as to the result to be achieved but shall leave to the national authorities the choice of form and methods. They shall not entail direct effect.' See also *The Amsterdam Treaty: a comprehensive guide* @ http://europa.eu/scadplus/leg/en/lvb/a11000.htm, (last visited Sept. 5, 2006).

[62] Digital Civil Rights in Europe. 'Council adopts decision on attacks against information systems' @ <http://www.edri.org/edrigram/number3.5/attacks> accessed May 23, 2006.

should be at least between one and three years of imprisonment in cases involving illegal system interference and illegal data interference. Art. 7 (which also includes illegal access to information systems under Art. 2(2) increases the criminal penalty between two and five years of imprisonment when committed within the framework of a criminal organisation.

Member States are required to implement this Framework Decision by 16 March 2007 (Art. 12(2)). Although the Framework Decision harmonises the laws of the member states in the area of attacks against information systems several limitations exist, including:

i. Framework Decision applies only to Member States of the European Union – the Framework Decision is restricted to Member States. This in turn limits the effectiveness of the Framework Decision because spyware is a global problem not confined within the European Union.

ii. Implementation of the Framework Decision is left to the Member States, which decide how the Framework Decision is transposed in their national laws. There is the potential for differences in the way Member States implement the Framework Decision. The problem is further exacerbated when such attacks on information systems can be transborder in nature.[63] Art. 10 contain a section on jurisdiction and Art. 4(4) deal with cross-border offences. However, it leaves it to the Member States to cooperate and decide which of them will prosecute the offenders. Although this is a good starting point, it is unclear how this will work in practice.

iii. The Framework Decision should be concerned with the technical weaknesses and not merely to criminalise or impose prison sentences.[64]

iv. The judiciary should be given sufficient information to educate themselves about the types of spyware available. They should not rely upon the information being provided by litigants and their lawyers. Failure to provide such education to the judiciary is likely to perpetuate the problem even further.

4. 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*).[65] But what of 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.[66]

[63] P. Van de Velde. 'EU Council takes action against attacks on information systems' @ <http://www.twobirds.com/english/publications/articles/EU_Council_takes_action_against_attacks_on_information_systems.cfm> accessed May 23 2006.

[64] A. Mueller. In: Digital Civil Rights in Europe. 'Council adopts decision on attacks against information systems' @ <http://www.edri.org/edrigram/number3.5/attacks> accessed May 23, 2006.

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

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

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"][67] the Stored Wire and Electronic Communications and Transactional Records Act [hereafter "Stored Communications Act"];[68] and the Wiretap Act.[69] Unfortunately, none of these three acts were designed to address the issues presented by spyware, and each have their significant drawbacks.

Under the CFAA,[70] 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.[71] An alternative possibility would be for the individual to claim the loss of personal data exceeding the $5,000.00 limit.[72] 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.[73] 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.[74] The damage threshold eliminates the CFAA as an avenue of redress for most consumers.

Under the Stored Communications Act,[75] it could be argued that spyware violates the Act by collecting personal information from an individual through a communication

[67] 18 U.S.C. § 1030 (2000 & Supp. 2004).

[68] See 18 U.S.C. §§ 2701–11 (2000 & West Supp. 2005).

[69] The Stored Communications Act adopts the definitions included in the Wiretap Act. Id. § 2711(1) (Supp. 2004). Under the Wiretap Act, an "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Id. § 2510(15). Under such a definition, an individual's home computer qualifies as an electronic communication service because it has the ability to send or receive electronic communications.

[70] See note 69.

[71] See, for example, the Dell Inspiron XPS, a gaming notebook computer priced at $2,828 at www.dell.com (last visited Sept. 20, 2005). Gaming computers, because of their advanced graphics and other attributes, are among the most expensive.

[72] See Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 681 (E.D. Tex. 2001) (holding that at least one protected computer must have an aggregate of over $5,000 in damage for a class to be certified). Once the class can find one protected computer, all injured class members may bring their claims, even if their individual damages are less than $5,000.

[73] See 18 U.S.C. § 1030(e)(6).

[74] Ibid.

[75] See note 70.

without that individual's consent. The Act specifies a private cause of action to protect individuals in their privacy.[76] 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.[77] 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.[78]

The Wiretap Act 2004 would seem to be the best avenue to address spyware.[79] However, unlike the Stored Communications Act, courts have limited its provisions to apply only to the interception of electronic information in transit.[80] The Wiretap Act was designed not only to protect digital communications, but to protect telephone calls over traditional networks.[81] 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.[82] The Wiretap Act while providing some legal viable recourse for the user does not provide a comprehensive legal 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;[83] and intrusion upon seclusion.[84] Neither common law theory has proven particularly successful.[85] 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.[86]

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

[76] A. Blakley, D.B. Garrie & M.J. Armstrong, see note 37.

[77] Once again, the Stored Communications Act refers to the Wiretap Act for its definition of electronic communication. In the Wiretap Act, electronic communication includes any data transmitted “in whole or in part ... affect[ing] interstate or foreign commerce.” Id. § 2510(12). By its very definition, spyware seeks to acquire such data and transmit electronically to the spyware company for the benefit of a commercial enterprise.

[78] Ibid.

[79] See A. Blakley, D.B. Garrie, & M.J. Armstrong, see note 37.

[80] Wiretap Act, 2000 & WestSupp. 2004.

[81] D.B. Garrie, D.Harris, & M.J. Armstrong, see note 41.

[82] Ibid.

[83] Restatement (Second) of Torts § 218, 1965

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

[85] A. Blakley, D.B Garrie & M.J. Armstrong, see note 37.

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

the consumer or of businesses in addressing spyware. Courts must be creative in applying the law to these new situations.

5. 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.

5.1. Multi-Click Consent Agreements Analogous to Initialing Each Pertinent Point Respective to Data Mining Performed by the Software Provider

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.[87] For instance, "piggyback" spyware applications, such as Kazaa, 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

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

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[88] without the user's consent.[89] 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.[90]

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.[91] 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.[92] 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

[88] M. Bono, 'Are you aware of spyware on your home computer?' *The Hill* @ <http://www.hillnews.com/thehill/export/TheHill/News/Frontpage/102005/ssbono.html> accessed March 7, 2006.

[89] 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.

[90] World Health Organization, 'World Health Report 1999: Making a difference' In: Chapter 5: Combating the tobacco epidemic. Geneva: WHO @ <http://www.who.org/tob/> accessed March 3, 2006.

[91] G. Mahood. 'Canadian tobacco package warning system' (1995) 4 *Tobacco Control* 10–14.

[92] A. Blakley, D.B. Garrie & M.J. Armstrong, see note 37.

help ensure that perpetrators who mine personal data without informed consent are brought to justice.

5.2. Potential Non-Statutory Solutions

While the international community is increasingly regulating activities on the Internet with promising statutory laws,[93]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 Data Protection Directive of 1995, 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.[94]

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.

6. Conclusion

While the U.S. and the E.U. do not comprise the entire international community, they would be a good starting point for addressing the spyware issue. By remedying the legal infrastructure in the U.S or the European Union, irrespective of the fundamentally different perspectives regarding digital privacy, it would provide a great starting point in addressing the global problem of spyware by providing 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, the challenge confronting countries around the world to protect their citizens' personal information will only increase. Spyware is not bound to a particular member state of the E.U. or a particular state in the U.S., in fact, spyware is borderless.

[93] M.C. Rundle, 'Beyond internet governance: the emerging international framework for governing the networked world' @ <http://cyber.law.harvard.edu/home/2005-16>accessed January 24, 2006.

[94] C. Nesson, A. Marino, & R. Kent. 'Privacy' @ <http://cyber.law.harvard.edu/ilaw/mexico_2006_module_3_privacy> accessed January 24, 2006.

The Framework decision fails to protect the citizens of Europe. The framework does not forbade spyware and the like from being used against European citizens as a whole. Even if Europe were to construct a unified anti-Spyware regulatory set, it is unlikely to protect their citizens. The main reason is that the technology driving spyware technology can be launched from countries (outside the EEA) where there is no legal reciprocity or jurisdiction available to the citizens of Europe. Of course, even if such reciprocity were available the average European citizen is not likely to have the necessary fiscal recourses to prosecute a transnational spyware perpetrator. Therefore, the governments of Europe acting alone will not be able to provide an effective countermeasure sufficient to protect their respective citizens.

An alternative solution to the spyware issue is not at a country level, but rather a global level. For example, perhaps the U.N. or the OECD can somehow be utilized to create a global information privacy framework as in the case of data protection.[95] Of course, any solution would never apply to a governmental actor, but only to 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 these emerging technologies on a regular basis because, by educating those tasked with interpreting the laws, fewer judicial loopholes will be created. For instance, if judges were better educated with respect to how the Internet operates as whole, it certainly would have improved the development of the law as applied to spyware and other internet data mining technologies.

[95] See the *Montreux Declaration* @ <http://www.libertysecurity.org/IMG/pdf/montreux_declaration_eng.pdf> accessed May 23, 2006.