INTRODUCTION: CREATING LEGITIMATE DIGITAL PRIVACY RIGHTS FOR INTERNET USERS

Daniel B. Garrie[1]

Privacy has become a complex legal issue as technological advancements have created a multitude of ways, both physical and digital, that one's privacy rights can be violated. Although the Supreme Court has declined to recognize a constitutional right to digital privacy, the increasing pervasiveness of digital privacy intrusions may encourage the Court to find that a right to digital privacy exists within the penumbra of rights established by the Constitution.[2] The lack of protection for digital privacy rights, whether oral or written, presents a wide range of novel challenges to our existing legal and social structures. This "privacy issue" of the Rutgers Journal of Law & Urban Policy explores the dichotomy in treatment between physical and digital privacy rights through several different articles, each of which provide unique perspectives on physical and digital privacy rights.

The Internet has revolutionized the way people interact, communicate and work. While the Internet has greatly increased our ability to communicate, it has also created numerous threats to the privacy of its users. Nowadays the exploitation of a person's digital information, including bank account numbers, credit card numbers and social security numbers, can lead to privacy invasions that are more invasive than physical privacy violations. The Internet's main culprits are data mining technologies that intercept and record information input by end-users. These technologies have appeared in numerous forms, including cookies, adware and spyware. The most insidious culprit is spyware, which has

[1] J.D., Rutgers University School of Law, 2005 with a focus on Cyber Law Litigation; M.A. Computer Science, Brandeis University, 2000 with course work in Artificial Intelligence; B.A., Computer Science, Brandeis University, 1999. Over the past eight years Mr. Garrie has worked with the Department of Justice (DOJ) and other large corporations as an Enterprise Technical Architect, focusing on web-enabled enterprise systems.

[2] *See generally,* California v. Acevedo, 500 U.S. 565, 581-585 (1991) (Scalia, J. concurring); Wolf v. Colorado, 338 U.S. 25, 27 (1949) (finding that the right of privacy is protected in the fourth amendment and also noting that it can be applied to the states via the due process clause); Angel v. Williams, 12 F.3d 786, 790 (8th Cir. 1993); Young v. Jackson, 572 So. 2d 378, 484-486 (Miss. 1990) (holding that other people may not invade the privacy zone without the person's consent); Norman-Bloodsaw v. Lawrence Berkeley Laboratory, 1998 WL 39209 (9th Cir. 1998) (finding that the constitutional right of privacy includes the right to choose not to disclose personal medical information in order to protect confidentiality).

led to violations of individuals' digital privacy rights (e.g., unauthorized reading of one's personal e-mails), identity theft, credit card and bank account theft, and loss of proprietary business information.[3]

Spyware is a growing epidemic that causes notable monetary damage to infected personal and corporate computer systems. Spyware's victims in the United States are deprived of a straightforward legal cause of action to obtain relief; instead they must patch together a web of complex federal statutes and state common law theories.[4] While some consumers and businesses may indeed find sufficient remedies through this patchwork system of laws, most spyware has been able to bypass any criminal or civil liability.[5] Country-specific statutory solutions have proven to be ineffective at impeding the propagation of spyware and other data mining technologies. A more viable solution is for countries to join together to implement uniform digital privacy protection laws that significantly improve national and international digital privacy remedies.

A potential statutory solution would be to require all spyware software to include a two-part End User Licensing Agreement ("EULA"). The EULA would require both a general acceptance of the terms by the end-user as well as specific acceptance at all points where access is granted to the end-user's personal information. The terms of this agreement and the extent of data that can be mined should be presented to the user in plain language that can be understood by a layperson.[6] It is imperative that the user be provided with instructions

[3] *See*, Stephen Shaw, *Mozilla, Opera and Firefox: Protecting Your Law Firm against Internet Security Issues*, 16-Jan. S. C. LAW. 26, *29 (2005) ("The e-mail usually provides the user with a link to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security and bank account numbers, that the legitimate organization already has. The most common of these is an e-mail appearing to be from a bank or credit card company. The return address on the e-mail appears to be from a bank. The contents of the e-mail look official. The Web page to which the user is directed looks familiar. However, scam artists create both the e-mail and the Web page, and all information entered is collected for nefarious purposes.")

[4] *See*, Alan F. Blakley, Daniel B. Garrie & Matthew J. Armstrong, *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 Duke L. & Tech. Rev. 25, *29 (2005).

[5] *See generally*, Daniel B. Garrie & Shira B. Kaufmann, *Warning Software May be Hazardous to Your Privacy*, 1 LEGAL, PRIVACY, & SEC. ISSUES IN INFO. TECH., 249 (2006).

[6] The language of the EULA must be written with the understanding that the end-user is not a lawyer or a programmer. Therefore, any legal or technical language must be carefully defined in simple terms.

indicating that clicking the "accept" button is analogous to "signing on the dotted line."

A typical multi-click consent EULA would provide an overview of each section in plain English and require the user to click "ok" for each clause relevant to the transmission of their personal information to a third-party vendor, thereby signifying that they read and consent to that clause.[7] Each clause pertaining to the transmission of personal data should require a check box to be clicked. Thus, "piggyback" spyware applications, such as Kazaa, which operate by installing spyware applications that are invisible to the user, would no longer be able to embed provisions deep within complex, cumbersome, and generally unread EULA's that enable it to install additional spyware applications. [8] Instead, a multi-click EULA would bring each component to the user's attention and only permit installation *after* the user consents to the personal data that may be recorded. "Piggyback spyware" such as Kazaa will be greatly limited by a multi-click EULA because a majority of users will not consent to the software's installation once they are alerted to the vast amount of data that it mines from their personal systems.[9]

The multi-click EULA solution will also require spyware developers to store a user's multi-click consent form on their servers for as long as they use, sell, or collect the user's data. By compelling storage of the consent form, valid

[7] The EULA should also provide the users with examples of the explicit information that the spyware agreement enables the program to mine from their machines. While the EULA currently may state that information is mined, under current practice, it is unlikely that the users, even if they read the EULA before clicking through, can understand what data that is being appropriated, or the ramifications of its being mined. For example, a multi-click EULA should read: "By installing this spyware application, you are consenting to the transmission of personal information. This information includes the following . . . . . Examples of such data are as follows. 1. "Mary J. Jenkins", "07/05/1969", etc.

[8] *See* Alexander Macgillivray, Spyware, *Malware and Adware: A View From the Trenches – Powerpoint Slides*, 828 PLI/PAT 673, *688 (2005). I.Lan Systems, Inc. v. Netscout Service Level Corp., 183 F.Supp.2d 328, 338 (D.Mass. 2002) (enforcing terms of clickwrap agreement where assent was explicit and holding that clickwrap license agreements are an appropriate way to form contracts). "To be sure, shrinkwrap and clickwrap license agreements share the defect of any standardized contract--they are susceptible to the inclusion of terms that border on the unconscionable--but that is not the issue in this case. The only issue before the Court is whether clickwrap license agreements are an appropriate way to form contracts, and the Court holds they are. In short, i.LAN explicitly accepted the clickwrap license agreement when it clicked on the box stating 'I agree.'" *Id.*

[9] *See Id.* at *685- 89.

commercial spyware users will have evidence to defend their actions in response to claims that their software operated in a manner "invisible" to the end-user. This requirement also provides the judiciary with a mechanism to differentiate between unlawful spyware (spyware that installs on the end user's personal computer without the user's consent and monitors key-strokes, passwords and other data) and permissible spyware (data mining software that monitors pages viewed by visitors to a company's own website).[10] Courts will be able to easily distinguish between lawful and unlawful spyware because unlawful spyware will simply lack the user's consent in the form required by the statute.[11]

The third and final element of the multi-click consent requirement is a remedy for breaches of the law's provisions. To promote enforcement of this statute, it would be beneficial if a "civil enforcement" provision were created that provides significant civil damages to aggrieved individuals irrespective of their actual losses. A civil remedy will help ensure that perpetrators who mine personal data without informed consent are brought to justice.[12] Implementation of this remedy for the aforesaid multi-click consent requirement, at both a domestic and international level, would help realign the law to better protect digital privacy rights.

While amending the U.S. legal code would be a notable improvement over the current legal landscape within which spyware operates, it will not completely eliminate the spyware problem because spyware is a borderless pandemic. Spyware vendors can operate effectively from locations outside the reach of U.S. courts or its allies. Therefore, in order to effectively implement a multi-click consent EULA, a uniform consent clause should be developed to standardize a statement of intent to mine personal data at a global level. Until such a statute exists and is enforced globally, spyware vendors will continue to capitalize on different countries' laws.

The adoption of a multi-click consent requirement will allow the market's invisible hand to re-allocate resources in a manner consistent with society's desires. Consumers will use products offered by trustworthy data mining companies and will avoid those offered by nefarious companies. Data mining companies that refuse to abide by the statute will be sued by spyware victims until they comply with the statute. The end result will be the creation of a

[10] 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 (Daniel.Garrie@gmail.com).

[11] The EULA should also state that the software will be transmitting data over the Internet, perhaps incurring Internet data transmission fees on behalf of the end-user as well as subjecting the transmitted data to further interception by others.

[12] *See*, Daniel B. Garrie & Shira B. Kaufmann, *Warning Software May be Hazardous to Your Privacy*, 1 LEGAL, PRIVACY, & SEC. ISSUES IN INFO. TECH., 249 (2006).

legitimate data mining and harvesting industry as consumers gain the ability to limit the amount data that they authorize for public use.[13]

The data mining and spyware industries are likely to resist any such multi-click consent requirement. Spyware and data mining programs, however, should be treated like the cigarette industry in that consumers should, at the very least, be informed of the potential harm that they may incur by using the product. Even though cigarette manufacturers resisted warnings, many countries now require warnings for the physical health of their citizens. Similarly, countries should require multi-click consent agreements for the "privacy health" of their citizens. Like cigarette smokers, spyware users would still be able to use the products on their systems if they choose to do so. The only difference would be that 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.[14]

The adoption of a multi-tiered consent requirement will provide much needed protection for Internet users' privacy rights. It will protect the average user from "piggyback spyware" while simultaneously providing spyware victims with a remedy against unlawful spyware. Most importantly, it will provide Internet users with what they need most; the ability to choose which data to keep private and which data to expose to the public. For this reason, the legislature should consider enacting a multi-tiered consent requirement to protect its citizens from unauthorized invasions of their digital privacy.

[13] The adoption of this solution could also create a market for different kinds of Spyware that mine different types of data. In this way, consumers could select freeware and shareware programs based on the capabilities of the bundled Spyware and the consumer's valuation of the data that would be mined.

[14] *See*, Alan F. Blakley, Daniel B. Garrie & Matthew J. Armstrong, *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 Duke L. & Tech. Rev. 25, *29 (2005).