An Analysis on Spyware Law SB 1436 (November 2004)

By Claudia Fong, Wallace Hung, Kartik Markandan

***Abstract* – This paper analyzes the California Senate Bill 1436 - Consumer Protection Against Computer Spyware Act. The different classes of spyware are examined. Then, the strengths and weakness of this bill are assessed by defining what each of the amendments cover and by pointing out what they do not cover.**

***Index Terms* – spyware, adware, SB 1436, software**

I. INTRODUCTION

Due to the flooding of spyware over personal computers that are attached to the internet, it has become a crucial problem. According to EarthLink, an ISP provider and creators of SpyAudit, spyware scanner has reported that there are on average 26 spyware on each personal computer scanned [1]. They also report that ninety-percent of all the personal computers in the internet have has some form of spyware on it [1]. Spyware has compromised user's privacy and also decreased the consumer's confidence in securing their data when connected to the internet. Hence, legislators have decided to put forth bills in the senate to stop the spread of spyware. In this article, we will analyze the Senate Bill 1436 which was proposed and legislated in the State of California. This bill is quite important and unique because it one of the first bills that was legislated in the country against spyware [2].

II. DEFINITION OF SPYWARE AND CLASSES OF SPWARE

Spyware can be defined in many ways. Stefan Saroiu, Steven D. Gribble, and Henry M. Levy broadly define spyware as a software that collects information that is available on a computer, and forwards this information to a third party [3].Most of the time, information is transferred without any notice from the computer's user [5]. There are several risks that are associated with spyware. Not only that spyware can appropriate resources of the computer it infects, it can also alter functions of existing applications, and for most of the time, benefits a third party. Apart from that, spyware is commonly used to transmit information about a certain user's behaviour and compromise the user's privacy. Another major concern is that spyware can detract from the usability and stability of a user's computing environment, thus having a potential to introduce new security vulnerabilities to the infected host. Since the use of internet is growing rapidly, spyware continues and will be a future security threat and a threat that cannot be ignored [6].

Stefan Saroiu, Steven D. Gribble, and Henry M. Levy divide spyware into many classes. We look at each of these classes in order to fully understand and appreciate the broad nature of spyware software that are available in cyberspace.

Cookies are small pieces of state stored on individual clients' Web browsers and can only be retrieved by the Web site

that first stored it. But since many Web sites use the same advertisement providers, they can track the behaviour of users across many sites [3].

Web bugs are invisible images that embed on Web pages. Advertisement networks usually contract with Web sites to place Web bugs on to their pages. Both Cookies and Web bugs rely only on existing Web browser functions and have no code of their own, thus they are just passive forms of spyware [3].

Browser hijacker is a type of spyware that attempt to change a user's Web browser settings, like modifying the start page, search functionality and other different settings. In order to predominantly affect Windows operating system, hijackers can install a browser extension, modify Windows registry, or replace browser preference files [12].

When Keyloggers were first introduced, they were originally used for recording keystrokes of a user so that to find passwords, credit card numbers and other sensitive information. But now, Keyloggers have been used to capture logs of Websites visited, instant messaging sessions, windows opened and programs executed.

Track is a generic name for information recorded by an operating system or application recorded by an operating system or application about actions the user has performed. Some examples of a track would be lists of recently visited Website maintained by most browsers and lists of recently opened files and programs maintained by most operating systems. Though tracks are typically innocuous alone, they can be mined by malicious programs and be potentially harmful [3].

Malware is a variety of malicious software that includes virus, trojan horses, worms and automatic phone diallers [4].

Spybot, a prototypical example of spyware, monitors a user's behaviour and collect logs of activity in which would be transmitted to a third party. The collected information include fields typed in Web forms, lists of email addresses to be harvested as spam targets and lists of visited URL [12].

Adware is a software that displays advertisements tuned to the user's current activity and can report aggregate or anonymized browsing behaviour to a third party[4].

III. DISCUSSION OF CALIFORNIA'S SENATE BILL 1436

Because the word "authorized user" is used extensively by the Senate Bill, before discussing the bill, it is important to declare what it means. Senator Murray the author of the bill defines, "authorized user" as a user who has leased the computer or authorized by the owner. It does not cover those who have been authorized to use the computer through a license agreement [2].

a) The bill states that software cannot change the homepage of the authorized user, the default provider or web proxy that the authorized user uses to search the internet. Furthermore, the bill declares that software cannot change the security settings of a browser to acquire information of the user or to harm the user.

This ruling partially defines and regulates against a class of spyware known as browser hijackers. The law fails to define software namely hijackers, that alter the search functionality or alter the links in a page, so that it points to another web page. Consider the case of software such as TopText, which hijack the links on a webpage by redirecting the links to a

competitor's webpage. This problem is one where the principle of trusted path is violated, because a user expects the link to lead to information that is related to the web page they are visiting. Thus, when they are led to another page or are shown information contrary to what they are expected, the principle of expected ability is also violated. At the end, user might not trust the web page and potentially dooming the business [5].

Another problem with this ruling is the difficulties that arise when one tries to enforce it. An obvious way that one might tackle this problem is by charging companies who use this browser hijacker. But, the problem with this approach is that, an attacker could create some kind of software, pretending to be working on behalf of a company, and get that particular company into trouble. This is really a question of non-repudiation. Take for example the case of porn company which uses a browser hijacker to advertise its products. How can we prosecute this company for using a browser hijacker, when the company could simply deny that they authorized the software, and instead, blame it on their competitors for creating that software in order to get the company into a legal wrangle.

b) The bill legislates against the form of keyloggers who record user information and transmit them to another user or computer. Personal Information includes a user's name, credit or debit card numbers, social security number, passwords or pin, account balances, overdraft history, payment history, history of websites visited, home address, work address and a record of a purchase or purchases made by the user.

Prosecution against keyloggers could be as difficult as it is against browser hijackers. The most important point to understand is that many users do not know the occurrence of loggers transmitting their keystrokes. Furthermore, even if one were to somehow able to locate the keylogging program, it is still difficult to find out who planted it in the first place. One approach to solving this problem might be to record the IP of the computer to which the information is being sent to. But an attacker could simply use a set of computers or zombies[i] as means to amass the information [6].

c) SB 1436 states that software should not record Web sites visited by a user without the user's permission [2]. Yet cookies are used by websites to identify the client to the website. This is because cookies are mechanisms that enhance the usability of a website. The website uses a cookie to track user preferences, and cookies are used to eliminate the need to fill out forms over and over again or to re-register again. The path of least resistance [7] tells us that consumers will choose cookies to enable them to do their tasks faster. Unfortunately, there is a penalty to pay for this. Cookies can be used by advertisers to track your preferences. In fact, there are some cookies that send information to both the web server and the advertisers. Thus, advertisers could potentially have information on what a consumer typed at a given site along with his or her email. So do monitoring user actions through cookies violate the law? The answer is no, because a user has the right to enable or disable cookies on one's browser. In some browsers the default setting is to enable cookies, therefore violating the policy of explicit authorization. The correct default option should be to disable cookies.

Another class of passive spyware is Web Bugs. When combined with cookies

this class of spyware can be used by advertisement providers to monitor a user's behavior. In fact, one could record the IP of the authorized user along with the information that the user uses to fill out web forms. This bill does not regulate against Web bugs [8].

Another example would be Intel Pentium III. It has an electronic serial number that could be tracked when logged onto the Internet. This would allow "snoopers" to track the surfing patterns of users, associate the specific names of the users to the CPU identification numbers, and sell the information to the market [6].

(d) SB 1436 addresses the issue that there must be a way to prevent the installation of software or if the software is installed, then it can be removed easily without fear of reinstallation or reactivation [2]. Stefan Saroiu, Steven D. Gribble, and Henry M. Levy report that spyware is often installed in a system without user's permission. This clearly shows a violation of the law of explicit authorization [3]. Consider the case of Gator, an adware created by Claria, attached along with Kazaa. Benedelman reports that Gator has a 56-page long document that comes along with every Kazaa installation [9]. Having this 56-page long document is obviously a deceptive technique. The users of Kazaa would be confounded with so much information that they will just click accept on each and every page without fully reading or understanding what they have agreed to have accepted. This is a direct application of the path of least resistance [7].

In order to combat this situation, we believe that the law should tell the adware company to clearly define in bold letters that they are installing an adware on the computer. They should also warn the user that an adware could cause a sizable delay in their daily computation. It is also essential for the company to clearly state the requirements to the user before downloading takes place.

Once spyware is installed the user for the most part is hard to identify Spyware files. Thus, a user has very little control of his or her system. The problem lies not only with spyware, but also with the operating system. Today's operating systems violate the principle of expressiveness. There is no option for a user to request that no spyware be installed inside his or her system. Therefore, the law alone will not suffice in protecting users against spyware. The operating system support is also needed.

(e) The bill also governs against misleading practices. For an example, when a user declines to install software, it will still continue to install into the computer. It also governs misrepresentation of software, such as informing the user that the software is needed for security or privacy reasons. Take the example of Windows 98. When it came out to the market, there was a feature during the registration process that prompted the user on whether or not the person wished to send system information to Microsoft. The button did not work properly and information was sent to Microsoft no matter the selection made was a yes or a no. Here, user has no right to choose at all. This violates the principle of expectability, a common practice among spyware. In fact, Grokster, a file sharing application, also installs software even if the user presses cancel [9].

(f) The bill states that the software cannot disable an anti-spyware, anti-virus software installed on the computer. This is an important regulation since spyware usually have mechanisms for self-updating.

Consider the case where the user could have potentially agreed to have software installed into his or her computer. He or she might have even agreed to future software updates. The software update might in the future decide to disable a feature of the anti-spyware or anti-virus software on the computer without checking with the user. The owner of the spyware could simply claim that the user had agreed to use the spyware and that the spyware had to disable the anti-spyware or anti-virus software to run itself.

(g) According to the bill it is illegal to transmit e-mail or a virus from a computer unless initiated by the authorized user. Thus, one cannot use to send spam to other users. Note the CAN-SPAM act states that one must have the postal code and return address and a way to opt out of receiving SPAM [10]. This portion of the bill illegalizes SPAM sent to another user without the awareness of the authorized user. This rule also prohibits the proliferation of malware in cyberspace.

Here, we can see one idea from computer security policies and it is availability. Because availability refers to the ability to use the information or resource desired, when the attacker wish to send any malware or e-mails, they are violating the law because most of the time, the receiver were not aware of such mails and did not give permission for the attackers to do so. Also, we can see that the attacker is violating the policy of authentication. The meaning of authentication is to show who you are, but most of the time when junk mails or virus are transmitted, the attacker would gather a bunch of mails and use those mailing address to send the virus to other mailing addresses on their mailing list. The attacker is not binding their identity to the mails that they are sending. But this bill is only a statement of what one cannot do, there are no real actions taken to stop or prevent these attackers from committing the crime.

(h) The bill stipulates that it is illegal to use software in order to use a consumer's modem or internet to incur financial charges. Here, we can again see the idea of availability. The purpose for this law to be posted is to stop attacker from trying to use other people's modem or internet so that they could dial expensive phone services and cause damage to the victims. Obviously, the attacker did not receive any permission from the victims so that they are allowed to use the victims' modems. Perhaps because of the difficulties in accessing someone else's modem considering that it would be easier to track the attacker when the crime is committed, violations of this amendment is not as common as the one above.

(i) The bill declares that it is illegal to flood the computer with ads with the knowledge that a user cannot close those ads without exiting the browser or shutting off the computer. This amendment is directed at practices of adware. Adware is fast growing industry with Claria, the parent company that owns the adware Gator, boasted 2003 net profits of $35 million on sales of $90 million [11]. Other problems with adware as reported by Stefan Saroiu, Steven D. Gribble, and Henry M. Levyare that they have weakness that might allow viruses or worms to propagate themselves using this software. SB 1436 should have declared that Adware companies must make their software as secure as possible. The mistakes these companies are making arise from not addressing the principle of least common mechanism which lead to non-

secure channels along which attackers can embed their malicious software [4].

IV. CONCLUSION

Senate Bill 1436 provides a good starting point in the fight against spyware. But as pointed out in the analysis of each amendment of the law, there are questions regarding how the law will be prosecuted and how we can enforce it on the internet. Another problem that arises when we try to enforce such a law is the fact that some of these problems arise out of poor usability techniques that have been employed by the operating system. As a result, laws alone will not be the answer to preventing the proliferation of spyware in cyberspace. Furthermore, the law has very little to say about the practices of adware. One should note that the SB 1436 applies only to California, but it provides, legislators of other states, a model on which they can build upon.

REFERENCES

[1] *Earthlink Spy Audit*, EarthLink Media Relations, Available: http://www.earthlink.net/spyaudit/press

[2] California State Senate, *Senate Bill No. 1436***,** CHAPTER 843, September 28, 2004, pp.1-6. Available: http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1436&sess=CUR&house=B&site=sen

[3] Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, *Measurement and Analysis of Spyware in a University Environment*. Washington, DC, pp.1-13.

[4] Matt Bishop, *Computer Security: Art and Science*, Addison Wesley Professional, 2002.

[5] Goth, G., *Spyware: Menace, nuisance, or both?* Security & Privacy Magazine, IEEE, Volume: 1, Issue: 3, May-June 2003 pp.10 – 11.

[6] Warren Harrison, *User Confidence--and the Software Developer,* Software, IEEE, Volume: 21, Issue: 6, Nov.-Dec. 2004 pp.5 – 8.

[7] K. Yee, User *Interaction Design for Secure Systems* pp.1-21.

[8] Cherry, S.M, *The illusion of web privacy*, Spectrum, IEEE, Volume: 41, Issue: 4, April 2004, pp.56, 58 - 59.

[9] Benjamin Edelman, *New and Notable* - Gator's EULA Gone Bad, November *29, 2004*, Available: http://www.benedelman.org/

[10] FTC, *The CAN-SPAM Act: Requirements for Commercial Emailers*, Federal Trade Commission for Consumers, 2004, Available: http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm

[11] B. Elgin. *Guess What – You Asked For Those Pop-Up Ads*, BusinessWeek Magazine, San Mateo, Califonia, June 28, 2004.

[12] Win Treese, *The state of security on the internet,* Volume 8 , Issue 3, 2004, pp.13 – 15.