Current ethical issues in spyware course work

Business, Company

Introduction

Over the years the growth and development of the internet has brought many opportunities for businesses and individuals to gather personal information about other users and to direct their advertising at these people. However, the means by which these things are done give rise to many ethical issues. For one thing, there is the question of whether an individual's browser history is his or her private property, or is it something which others should be allowed to share? Another issue is at what point are companies being simply unethical? At what point are they breaking the law? At what point should they be considered to be breaking the law? These are the ethical questions that will be discussed in this article.

In considering these issues, it is important to understand the methods, which are used. There are two main software types that will be considered in the paper; spyware and adware. Spyware is defined as computer software that collects personal information about a user without their informed consent, while adware is any software package, which by design plays, exhibits, or downloads promotion substance to a computer after the software is inaugurated on it or while the application is being utilized. There is a view that spyware should be considered to be Malware, software designed to infiltrate and damage a computer. This is something of a gray area since most types of spyware are designed primarily to gather and relay information rather than to directly harm a computer.

In my opinion, it is therefore misleading to describe these programs as malware. This does not however mean that I consider them ethical. In fact,

both spyware and adware share the same central ethical issue, the fact that users are not informed of them being downloaded or installed on their system. Many of these programs are automatically downloaded when users visit a webpage; others ‘ piggyback’ on other programs, which may be downloaded. Either way the user is not made aware of the software’s installation so I do not see that there can even be a question of right or wrong.

There are a variety of methods by which spyware can accumulate information on a system. Some may log keystrokes on the users’ keyboards to retrieve password information, other more sophisticated packages can scan all files and folders on an affected hard drive. These are both very intrusive and would certainly be considered malicious software. What do distributors of spyware wish to gain by gathering information in this way? Alternatively, more precisely is there an ethical argument in favour of it? Certainly, there are many unethical possibilities. For instance, a hacker could use spyware to gain security information about a system, even passwords. If the program discovers security weaknesses then perhaps a ‘ back door’ could be found which the hacker might use to gain access. A company may be interested in gathering browser information or information on other software packages, which are on a given computer. For instance it may be of interest what other kinds of software are being used by people who use the software that a given company provides. This information could be used as inspiration to further develop their own product. This manner of gathering the details however, that is without the users knowledge undoubtedly unethical in my opinion, regardless of how ‘ harmless’ the software may be.

In the end, the installation takes up space on the users' hard drives and it uses system resources to operate, potentially slowing the computer. At the extremely least this is an inconvenience. I would raise the question ' if it is ethical and the people using the software believe it to be ethical then why hide it?'

As for adware, this software is designed specifically for advertising so it definitely cannot be considered malware. It is downloaded onto individual computers or networks in the same way as spyware but is less interested in information about the users of the system. Instead it concerns itself with advertising to the user. Generally this is done by way of pop ups which appear on the screen of the computer when a given action is performed by the user such as running a specific program or visiting a web page etc.

Some forms of spyware have similar properties to adware. The distinction is that adware simply displays pre-programmed advertisements on the screen (or link to sites which send advertisements) whereas the spyware programs will use information gathered about the user to display advertisements which in theory will appeal more to that specific user. Whether it is adware or spyware, all these programs use system resources and memory, slowing an affected computer. However, the biggest problem with advertising software for the user is the inconvenience to the user. Often, the pop ups need to be closed by the user, thus in theory they are forced to read the advert. In practice, however these adverts just get in the way of what people are trying to do, a trait, which can be very frustrating for users. The ethical issue of adware therefore comes down to a matter of convenience. On the one hand,

the software is harmless to the computer and is therefore not illegal, but on the other, it is intrusive in its own way.

Problems associated with spyware

Spyware programs frequently cause noteworthy dilapidation in system performance. Significantly slowed computer performance is the number one spyware-related complaint that computer manufacturer Dell receives, accounting for more than a quarter of all spyware-related complaints as of April 2004. Spyware can even cause computers to crash. Microsoft reported that 50% of its customers' computer crashes are traceable to spyware. Spyware may use so many system resources that users are no longer able to use their mouse, and their cursors freeze. 1

Spyware causes computers to malfunction in part because of the large number of tasks, or operations, it commonly forces a computer to run. Spyware can also account for as many as 600 to 800 operations running simultaneously on a user's computer, as contrasted with the normal number of perhaps 30 or 40 operations running. 2 These system degradation effects were described as cumulative over time, and increase as additional spyware programs are installed. 3

Another adverse impact mentioned is that spyware can result in loss of Internet access. 4 The explanation given for this result is that some spyware inserts itself into the chain of connections by which a user's computer connects to the Internet to watch what is being transmitted over that connection. Subsequently, when the spyware is found and deleted, it leaves

a gap in this chain, thereby preventing the consumer from reaching the Internet.

It also be noted that removing spyware could also impose substantial costs on consumers and businesses. 5 In severe cases, if the spyware cannot be removed, the computer hard drive may have to be erased and reformatted. If so, all systems, programs, and files must be reloaded, a process that can take hours if not days. 6 If users have not backed up their data, this reformatting process can result in loss of valuable documents, such as tax returns or photos. 7

Some users have even found that it is less expensive to buy an entirely new computer than to pay someone to clean up a spyware-infected one. In other cases, users were reported to have cancelled their broadband Internet accounts and returned to dial-up access, because they believed the faster broadband connection made them too much of a target for spyware8.

Various privacy risks associated with spyware that vary in both scope and severity. These risks include the theft of personal information, monitoring of communications, and tracking of an individual’s online activity. Several experts have observed that the most serious privacy risks arise when spyware installed on a computer includes a “ keystrokelogger. 9” A keystroke logger captures all keystrokes that the user types on the computer keyboard, including passwords, personal information entered into an online registration form (e. g., a mailing address or telephone number), and financial information submitted as part of an online transaction, and the contents of emails or instant messages. 10 Although, at present, spyware

that includes a keystroke logger does not seem to be installed frequently, therefore it poses a risk of substantial injury, such as identity theft, when it does occur. 11

Businesses also face the risk that spyware will be used to access their information. The installation of spyware on a company's computer system could expose trade secrets and other confidential business information. It also could put the company at risk of compromising customer data in its possession, such as sensitive financial records, and lead to a loss of consumer confidence in conducting transactions online12. There is little hard data regarding the extent to which spyware has been used to obtain businesses' confidential or private information. Many companies apparently are aware of these risks and often have taken steps to protect themselves, which may have limited the instances of unauthorized access or their impact. 13 However, it should be noted that as spyware becomes more sophisticated, businesses might face increased privacy risks. To respond, companies may face increased costs in protecting confidential business information, including sensitive customer information.

It is also reported that some spyware programs have prevented users from downloading their Windows security patches or updating their anti-virus or anti-spyware programs. For instance, spyware may misdirect access requests and thereby prevent users from reaching the websites of McAfee, Lavasoft, Pest Patrol and other anti-virus or anti-spyware companies. 14 Some spyware will turn off users' firewalls and anti-virus programs. 15

Spyware that includes a keystroke logger can create security risks. Such software is designed to enable the person or entity who installed the keystroke logger to monitor remotely the activities and communications on a user’s computer. If the keystroke logging program is poorly written, it could be hacked into by persons other than the person who installed it, which would allow these unknown hackers to remotely record all of the activity on that computer.

LEGAL issues of spyware

The current laws handle those items connected to right to privacy and information operates proportionate to communications. The truth there are many actions, which happen on computers not overseen by present laws raises the query is it in opposition to the law to take data from an individual's computer without consent.

The realism is many or else frank companies with whom people do trade on the computer are deceitful in one significant area, which is the exploit of cookies to assemble information. Again, can this to be described as prohibited because there actually is not a body of legislation associated with computer problems. It appears morality and ethics have to limit the dissipated and unprincipled behaviours, which source computer problems however this is a very impractical outlook!

Pinching information from individuals’ office or home is unlawful and can direct one to a jail condemnation, however what about information taken from a computer, is this lawful? Some people agree it is legal, since a distinct law forbidding it does not subsist, while others say it does not matter

whether it is lawful or not since, there is no way to know the names of the spies. This is a factual declaration to a degree, but there have been both " white hat" and " black hat" hackers charged and sentenced of such crimes.

The acknowledgment of the nonexistence of suitable laws to thwart unlawful actions on the computer is an issue law schools are training law students for in the struggle against spyware assaults on computers. The right to privacy act does not envelop the act of placing spyware on an individual’s computer, which is competent of destructive effects on the computer and stopping the computer from operating correctly. Spyware, which damages the hard drive in computers, is prohibited based on ethical, moral standards however this is not adequate to avoid it from occurring.

Obliterating a person's hard drive or any element of a computer is destroying or demolishing the possessions of another. An individual cannot enter ones home and pinch a computer, nor can the individual take a mallet and shatter ones computer and up until now, the same individual can put a portion of spyware into ones computer and everlastingly obliterate it wholly or partially. The only action one can take is to purchase a new computer.

There are additional laws required and law students and professors will carry on raising questions associated with computer legislation for managing spyware and other forms of computer exploitation. The administrations are starting to act by drafting laws, when their efforts pass into success, the apparently everlasting fight with spyware will progress. In the meantime, those who possess and utilize computers must rely on sincere companies to offer anti-spyware to fight the battle against spies for us.

How to detect spyware and protect privacy

The approaches to reduce unwanted spyware include user initiatives, technological approaches, industry self-regulation, and legislation. None of these approaches alone has been effective. Rather, battling spyware requires a combination of these approaches

User Initiatives

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

Technological Approaches

Technological approaches include anti-spyware software, firewalls, and spyware blockers. The market for anti-spyware software is still small, with $10-$15 million in sales, compared to the $2. 2 billion anti-virus software industry. Effective anti-spyware software should identify the spyware threat, provide an explanation of the threat, and allow the user to decide what to remove. To date, no anti-spyware utility can provide an impenetrable defence16 . Attracted to the potential to generate advertising revenue, professional programmers continue to refine spyware to make it difficult to identify and remove. Therefore, at least two anti-spyware tools should be used, as the first may not detect something that another tool does. Further, every network or PC that accesses the internet should have its own firewall.

Defensive spyware blocker software can also detect and stop spyware before it is installed.

Industry Self-Regulation

Most reputable technology providers feel that adherence to the following principles is crucial for adware providers17 : Clear and prominent notification presented to the user prior to downloads or data collection. Additionally, the EULA contains such notification. The user has the opportunity to accept the terms of the application for both access to the user's PC and to any communications between a user's PC and the internet. In addition, Adherence to all application laws and best business practices for internet business. The FTC is currently endorsing the use of self-regulatory measures as opposed to the introduction of legislation.

U. S. Legislation

The U. S. federal government is investigating the effects and legitimacy of spyware, with the FTC leading the charge. While legislation has been proposed at the federal level in the Senate and House of Representatives, some states have already imposed regulations. Spyware has not yet caused widespread public outcry because most users are unaware that their systems have been compromised. 18

Conclusion

Moral and lawful concerns connected with spyware call for a reaction. The form of that response will ultimately be determined by users themselves through their assessment of the ease and effectiveness of the various approaches to battling spyware. Will user protests ultimately be so strong as

to lead to legal legislation? While the concerns associated with the presence of spyware are clear, legislating spyware is difficult because the definition of spyware is vague. Passage of legislation has been slow because broad legislation could prohibit legitimate practices and stifle innovation. Protecting consumers' concerns has to be carefully balanced against the beneficial use of spyware as a legitimate marketing tool. Currently, there is not widespread awareness or understanding on the part of users as to the existence of spyware, its effects, and what remedies are available to defend against its installation or removal. As the prevalence of spyware continues to increase, escalating concerns of users regarding the acceptability of spyware will ultimately drive a resolution in balancing the legitimate interests of spyware installers with those of users.

Bibliography

Cushman, R. and Gilroy, R. J., 2007. Software program activation. Third ed. Bloomington: Indiana University Press.

Clyman, J. 2004. Antispyware: Adware and spyware area growing nuisance and threat, PC Magazine, 23(13): 82.

Gordon, T and Wood, R. 2003. Corporate manslaughter: new issues for hackers.

The Times, 3 Sep. p. 4b.

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

Turner, C., 2004. The Breton Woods proposal: an in-depth look. Computer Science Quarterly, 42(6), pp. 564-78.

Urbach, R. R., and Kibel, G. A., 2004. Adware/spyware: An update regarding

pending litigation and legislation, Intellectual Property and Technology Law Journal, 16(7)