WRITTEN COMMENTS OF RAY EVERETT-CHURCH
Spyware Workshop – Comment, P044509

It is my honor and privilege to submit these comments to the Federal Trade Commission (hereinafter, the "Commission") for consideration during their public workshop, entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software."

INTRODUCTION

In order to place my comments in an appropriate context, I wish to provide the Commission with some background about me. I am currently employed as Chief Privacy Officer for TurnTide, Inc., an anti-spam technology company. Since 1994, my work has focused almost exclusively on legal and policy issues surrounding the Internet and the implications for online marketing and advertising practices. I have advised an array of clients, including America Online, Aventis Pharmaceuticals, Comcast, Coremetrics, Ericsson, Household HSBC, Intuit, Kimberly-Clark, Microsoft, and Pharmacia, on a wide range of Internet advertising, online marketing, and Web site development issues. As a result of these experiences, I have extensive knowledge of current industry practices and business considerations arising from the design and development of Internet Web sites and other online marketing activities.

In recent years I have testified before committees of the United States Senate, United States House of Representatives, the Federal Trade Commission, and the California state legislature, on issues relating to consumer privacy, electronic commerce, and online marketing best practices. I am also a co-author of *Internet Privacy for Dummies* (2002) and *Fighting Spam for Dummies* (2004), both from John Wiley Publishing, in which my co-authors and I educate readers regarding online marketing and advertising practices which threaten the privacy of their personal information and/or present the risk of unauthorized collection, use, and abuse, of information about their online activities.[1]

Particular to the topic of spyware, my services have recently been engaged on an independent basis by L.L. Bean, Inc., Extended Stay America, Inc., TigerDirect, Inc., The Hertz Corporation, LendingTree, Inc., Six Continents Hotels, Inc., Inter-Continental Hotels Corporation, United Parcel Service of America, Inc., True Communication, Inc., Wells Fargo & Company, WFC Holdings Corporation, and Quicken Loans Inc., to testify as an expert witness with respect to marketing and public policy considerations arising in the course of litigation against Claria Corporation (formerly known as The Gator Corporation). Because that litigation is ongoing, and because the materials surrounding the litigation are subject to a protective order, I will confine my comments to facts that are clearly within the public domain and opinions drawn solely from my review of publicly available information about the business practices of companies in the spyware industry.

BACKGROUND ON SPYWARE

In my book, *Internet Privacy for Dummies*, my co-authors and I define spyware as any piece of software that gathers information and uses your Internet connection to send it

[1] I would like to thank my co-author, Dr. John Levine, for his assistance in preparing these comments.

somewhere else, without your explicit knowledge or approval. The most common types of spyware collect information about you and your activities on your own computer and send that data back to the software manufacturer or some other data-collection company so that the information can be used for a variety of purposes.

One of the first known examples of a spyware-type behavior was a feature built into Microsoft's Windows 95 operating system. As is often the case with new software, users are asked to register their software purchase with the manufacturer in order to obtain support and to "activate your warranty." But when Windows 95 asked users to register, the Registration Wizard did much more than send in registration information. It also scanned the user's computer to compile a list of all the computer's hardware and all the software installed on the machine, bundled up that information, and sent it back to Microsoft, all without telling users what it was doing. Despite a significant outcry from privacy advocates and legal experts concerned with anti-competitive uses for that information, Microsoft continued collecting this data. It did, however, modify the Registration Wizard to make transmitting the data optional during the installation process.

Following the Microsoft lead, many other software manufacturers capitalized on the idea to include spyware features in their software. For example, the popular music trading program Kazaa has long been known to install various types of spyware and other secondary applications which behave in ways that may not be clearly understood by consumers. For example, it was discovered in April 2002, that Kazaa secretly installed software of an advertising company called Brilliant Digital Entertainment which, according to the company, could turn every computer running Kazaa into a part of a stealth network controlled by Brilliant.[2] The company claims it will only use the network with users' permission. But if you installed Kazaa, you already gave permission: Buried in the software usage agreement is the line: "You hereby grant [Brilliant] the right to access and use the unused computing power and storage space on your computer/s and/or Internet access or bandwidth for the aggregation of content and use in distributed computing."

Another popular file sharing program called AudioGalaxy was discovered to quietly install a program called VX2. Like many types of spyware, VX2 reportedly generated pop-up ads "so that they appear to be coming from websites that don't actually serve the ads."[3] Indeed, pop-up ads are one of the most common characteristics of spyware, and in my experience working with consumers, many of the pop-up ads that annoy and frustrate consumers during their Web browsing experiences are indeed generated by spyware that has come to be installed on their computer, often without their knowledge or consent. By far, the most popular page on our Web site, InternetPrivacyForDummies.com, is the page describing various types of pop-up ads and how to deal with the software responsible for them.

The business model of many spyware companies is founded on delivering marketing messages on behalf of advertisers directly to consumers, through the wide-scale distribution of ad-delivery software to millions of consumers. Spyware companies achieve this distribution most

[2] John Borland, *Stealth P2P network hides inside Kazaa*, CNet News.com, April 1, 2002, at http://news.com.com/2100-1023-873181.html (visited March 17, 2004)
[3] Jeffrey Benner, *Spyware, In a Galaxy Near You*, Wired News, January 24, 2002, at http://www.wired.com/news/technology/0,1282,49960,00.html (visited March 17, 2004)

frequently by bundling the spyware application along with ostensibly "free" software packages, such as the music trading software applications Kazaa and AudioGalaxy, and through the other types of software, including various tools, utilities, and add-ons for other popular Web technologies (such as plug-ins for browsers or decoding software – called a "Codec" – for multimedia applications used to view video online).[4]

Because of consumer dislike for the concept of spyware and the pop-up ads that often accompany it, spyware creators have been forced to find creative, and often deceptive, methods of surreptitious distribution. A common process is one in which the spyware creators will engage in profit-sharing programs with the authors or distributors of the software which acts as the delivery vehicle for the spyware applications. These distribution incentive programs allow software publishers and Web site operators to get money for each time the spyware is downloaded onto a consumer's computer. This often creates a financial incentive for these distributors to get their software downloaded and installed by any means necessary, including through means that are without the consumer's clear knowledge and consent.

Once the software applications containing the spyware have been downloaded and installed on a user's computer, many of the spyware packages then begin communicating information about the usage habits of the computer user, including what Web sites they visit. Many spyware applications will use that information to occasionally generate pop-up advertising window, which displays an advertisement in a window that appears in a layer over the top of the content of the original Web site being viewed by the user. In some instances, spyware may also cause a window to "pop-under" the site being displayed, so that when the user eventually closes their main Web browser window, the pop-under is revealed.

While pop-up ads are intended to present adverting information to consumers, the result is often confusion and frustration on the part of those consumers inundated with unwanted pop-up ads. It is well-established across the Internet advertising industry that consumers hate pop-up advertisements.[5] According to a recent *New York Times* article, consumers are rushing to install pop-up blocking software in an attempt to be rid of this proliferating annoyance.[6] Indeed, pop-ups are so reviled that companies targeted by unauthorized pop-ups have taken steps to distance themselves from pop-ups generated by unaffiliated sources.[7] Moreover, advertisers themselves are beginning to rethink their own usage of pop-up ads, even going so far as, in the case of America Online, offering their own pop-up blocking software to block the ads they once so heavily relied upon for ad revenue.[8]

---

[4] For example, the Web site PC Pitstop lists several applications and one popular Codec containing spyware at http://www.pcpitstop.com/spycheck/default.asp (visited March 17, 2004).
[5] See, e.g., Denise Garcia, *Unpopular Pop-Ups Won't Stop,* Gartner G2 (December 2002); *Darn Those Pop-Up Ads! They're Maddening, But Do They Work?* Wharton School of Business, University of Pennsylvania, August 2003 at http://www.inc.com/partners/techstation/articles/popup.html (visited March 17, 2004)
[6] Saul Hansell, *As Consumers Revolt, a Rush to Block Pop-Up Online Ads*, New York Times, January 19, 2003, at http://www.nytimes.com/2004/01/19/technology/19popup.html (visited March 17, 2004)
[7] Stefanie Olsen, *Google distances itself from pop-ups*, News.com, January 29, 2002, at http://news.com.com/2100-1023-825507.html (visited March 18, 2004)
[8] Brian Morrissey, *AOL Pops Pop-Ups*, InternetNews.com, March 12, 2003 at http://www.internetnews.com/IAR/article.php/2108501 (visited on March 17, 2004)

One of the reasons that consumers are so often annoyed by pop-up ads is that research indicates that consumers engaged in many types of e-commerce transactions are highly goal-oriented and focused on their tasks. For example, Jupiter Research analyst Raj Dhinsa, who led a study of online banking Web sites, concluded that because online consumers are highly task-oriented (for example, 80 percent of online shoppers shop with a very specific product in mind), Web page designs must prioritize and quickly facilitate the most common banking interactions.[9] While Mr. Dhinsa's report did not directly discuss pop-up advertisements, the clear implication to be drawn from his research is that anything which distracts or disrupts a Web site visitor from the task which drew them to the Web site acts as an obstacle to overall usability of the Web site. Such a conclusion is supported not only by common sense but by other studies which concluded that 61 percent of consumers would make greater use of sites that utilize clear navigation designs without complex menus, windows, or other distractions.[10]

Drawing upon research such as that, many corporations expend significant amounts of money and personnel resources on designing and implementing their corporate Web sites. For example, Jupiter Research reported that companies with annual revenues of $500 million or more spent an average of $3.9 million in 2002 to develop and maintain their Web sites.[11] Similarly, Forrester Research found that the Fortune 1000 companies each spend an average of $2 million per year on Web site redesigns.[12] These high costs of Web site operations are forcing companies to pay much more attention to the design (and redesign) process to better manage the results of those investments.[13] The consequences of not taking such measures to perfect the user experience on Web sites have also been studied. For example, research indicates that Web sites run the risk of losing existing customers, or greatly diminishing their lifetime value, if the consumer experiences problems accessing the home page of their preferred Web site. According to a Jupiter survey, 46 percent of users have on at least one occasion been driven to alternative sites because of a problem upon reaching their preferred Web site.[14]

HARM TO THE COMPETITIVE ENVIRONMENT

In my opinion, each time an unauthorized advertisement pops-up over a carefully-crafted corporate Web site, the result is to devalue much of the expense and effort put into creating and perfecting the Web site. Further, it is my opinion that if a user's visit is their first to that Web site, the confusion created by a pop-up advertisement can destroy the all-important first impression of that Web site – and by extension, the first impression of the company – in the mind of the visitor. The end result is to fundamentally damage the brand name and future

---

[9] Raj Dhinsa, *Web Design: Formulating a Better Banking Home Page*, Jupiter Research (April 14, 2003)
[10] Stacey Herron, *Site Navigation: Differentiation and Customer Loyalty via Native Navigation*, Jupiter Research (June 28, 2001); Sarah L. Roberts-Witt, *Site Design as Business Decision*, PC Magazine (September 25, 2001) at http://www.pcmag.com/print_article/0,3048,a=12700,00.asp (visited March 18, 2004)
[11] See, e.g., Ken Allard, *Web Site Spending in 2002: Saving Money by Not Overspending*, Jupiter Research (December 20, 2001)
[12] See, e.g., Sari Kalin, *Mazed and Confused*, CIO Magazine (April 1, 1999) at http://www.cio.com/archive/webbusiness/040199_use.html (visited March 18, 2004); Paul Sondregger, *The Site Redesign Playbook*, Forrester Research (October 2003)
[13] See, e.g., Matthew Berk, *Web Site Usability: Maximizing Business Value Through Rigorous Management*, Jupiter Research (September 24, 2002)
[14] Ken Allard and Cormac Foster, *Testing Tools and Methodologies: How to Build a Failure-Proof Site*, Jupiter Research (January 19, 1999)

business prospects of the company whose Web site is obscured or otherwise affected by unwanted and unauthorized pop-up advertisements. The ultimate effect of unauthorized pop-up advertisements is to disrupt, and ultimately negate, the lengthy and costly efforts to which Web site operators go in order to presents a well-organized, efficient, and effective Web site presentation.

The return on the investment made in a carefully engineered Web site is inherently diminished when those efforts can be superseded, and indeed capitalized upon, by an unauthorized third party. I believe it is inevitable that an unchecked proliferation of spyware-generated pop-up advertisements could have the consequence of chilling investments in Web site quality and usability, particularly if those investments if they can be so easily vitiated by the practices of spyware creators and distributors. The ultimate harm done by a reduction in those investments is a predictable decline in usability for consumers and foregone business opportunities for companies.

With companies spending such large sums of money on creating Web sites, the next critical task of businesses, after making substantial investments in their Internet sites, is to drive users to those sites. For the world's best-known brand names, such as Coca-Cola, Ford, or Pizza Hut, both online and offline advertising form a critical part of their overall marketing and branding strategies. For the better part of a decade now, soda cans, billboard ads, and pizza boxes have featured Web site addresses in order to drive consumers to visit Web sites for entertainment, coupons, and other marketing and sales activities. Looking around the streets of any major city, one can see untold numbers of advertisements featuring little more than a company's Web site address. Even the license plates in the Commonwealth of Pennsylvania feature the official Web site of the Pennsylvania government, encouraging citizens to obtain information and services through the online medium.

For every company with a multimillion dollar advertising budget aimed at driving consumers to visit their Web sites, there are dozens or hundreds of companies for whom the online advertising medium represents their primary vehicle for driving consumers to their Web site. It has been estimated that companies spent $6.3 billion on online advertising in 2003, with steady growth in ad spending projected through 2008.[15]

It is my opinion that, fundamentally, the business model of spyware companies is inherently based upon free-riding on the investments made by other companies in developing and promoting their Internet presences. Many of the spyware applications being distributed widely today monitor the Web surfing behavior of consumers specifically for the purpose of generating pop-up advertisements when those consumers visit particular popular Web sites. Those spyware applications tend to deliver their pop-up advertisements only after a consumer has chosen to go to a particular Web site, often as a result of a costly advertising campaign that has led the consumer to seek out the site. At the precise moment when those advertising dollars are paying a dividend – namely, the arrival of an interested consumer – the spyware company delivers a competitor's message in a fashion that interrupts the consumer and obscures the Web site they intended to visit. This hijacking of a consumer's attention turns the idea of fair

[15] Gary Stein, *Online Advertising Through 2008: Paid Search Drives Modest Recovery*, Jupiter Research (August 28, 2003)

competition on its head, with the natural and inevitable result being to significantly chill investment in the promotion of Web sites and Internet commerce.

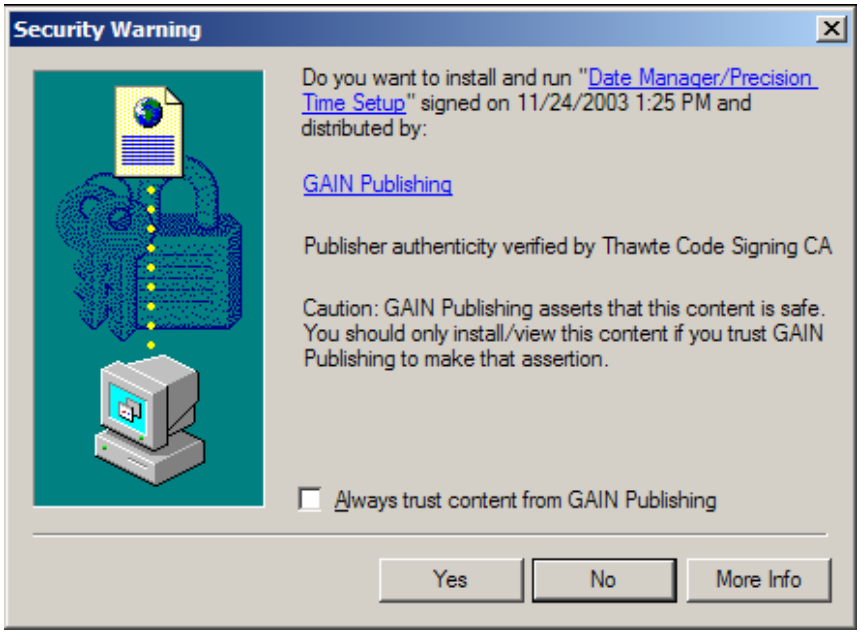
By analogy, it is not difficult to imagine the frustration experienced by the executives of a company that, as part of a coordinated marketing strategy,[16] might spend as much as $2 million for a 30-second advertisement during the Super Bowl – what AdForum.com calls "the most important advertising event of the year in the US"[17] – only to find that their investment has been usurped when unauthorized pop-up ads generated by a spyware application obscures viewing of that Web site with an advertisement for what could be that company's most hard-fought competitor. While one might expect the executives of the targeted company to be angry, one can also be assured that these same executives will have significant reservations before making such an investment again.

In this fashion, I believe that the practices of spyware-based advertising companies generally act to turn upside-down the notion of fair competition in a free market and allowing unauthorized parties to free-ride on the investments of others. The result is to, in effect, allow those advertisers who utilize spyware-based pop-up ads to supplement their advertising budgets with the investments made by those whose brands are targeted by the pop-up software. Through an unfair technological circumvention of the normal advertising process, these advertisers are given the ability to deliver their advertising based not on their own efforts and investment in brand identity and advertising presences, but rather upon the efforts, popularity, brand recognition, and investments of others. As a result, it is my opinion that the inevitable result of permitting one category of companies to usurp the brands and goodwill of another will cause businesses to reduce their investments in promoting and advertising their Web sites, resulting in less competitive information being presented to consumers.

SPYWARE OFTEN FAILS TO PROVIDE ADEQUATE NOTICE & CHOICE

In the course of my research for the book *Internet Privacy for Dummies*, I visited numerous Web sites distributing a variety of spyware applications. For example, upon visiting a particular Web site, I found one of the products published by GAIN, an affiliated entity of the Claria Corporation (formerly known as Gator Corporation), being deployed as an automatic download forced upon every visitor arriving at that Web site:

[16] Brian Morrissey, *Super Bowl Ads Use Web to Maintain Buzz*, InternetNews.com (January 31, 2003) at http://www.internetnews.com/IAR/article.php/1577621 (visited March 18, 2004)
[17] *Super Bowl Ads* (glossary entry), AdForum at http://ww0.adforum.com/help/glossary.asp#s (visited March 18, 2004)



This dialog box is generated by the Internet Explorer software to advise users that the Web site being visited is attempting to install a piece of software on their computer. Because it is a standard feature of Internet Explorer, the form and appearance of the dialog box is virtually identical in nearly every instance in which an attempt to install software occurs, regardless of the nature or function of the software being installed. As can be seen from the contents of that dialog box, there is no useful disclosure provided to consumers other than the name of the software being installed and the "distributor" of the software. It is in no way apparent from this dialog box that the end result of this installation process will be surreptitious user monitoring or pop-up advertising.

In the installation box reproduced above, I find nothing that provides enough information to permit an average user to make an informed choice regarding the ultimate functions of the software being installed. (It should be noted that the "More Info" button calls forth a brief explanation of why the Internet Explorer browser has alerted the user. There is no additional information regarding the software in the "More Info" window.) As an experienced user, however, I do recognize that in the dialog box, there are two sets of underlined words which function similarly to Web page-style hyperlinks and can be clicked. Doing so leads to a general Web site promoting the software. However, due to the design of the dialog box, the ability to click on those pieces of text will not be readily apparent to the average user because of the visual differences between a specialized dialog box and a typical Web browser window. In fact, during the course of my research into "spyware" for *Internet Privacy for Dummies*, I learned from speaking with many novice users that when they see a dialog box feature prominent "Yes" or "No" buttons, they make the assumption that those are their only choices at that moment.

If the user clicks "Yes," they are then presented with a quick series of similarly boilerplate-style dialog boxes, one of which appears to be a standard End User License Agreement ("EULA") of the sort displayed during the installation of virtually every piece of

software a user will experience in their computer-using careers. Buried within the details of the multi-page license agreement – which, by my count, is approximately 6,270 words long and consumes approximately fourteen (14) single-spaced 8.5 x 11 pages – is a disclosure regarding the behavior of the GAIN software. The word "pop-up" first appears four pages into that document. Because the EULA display window is so small, it can take as many as ten (10) mouse clicks to reach the first instance of the word "pop-up."

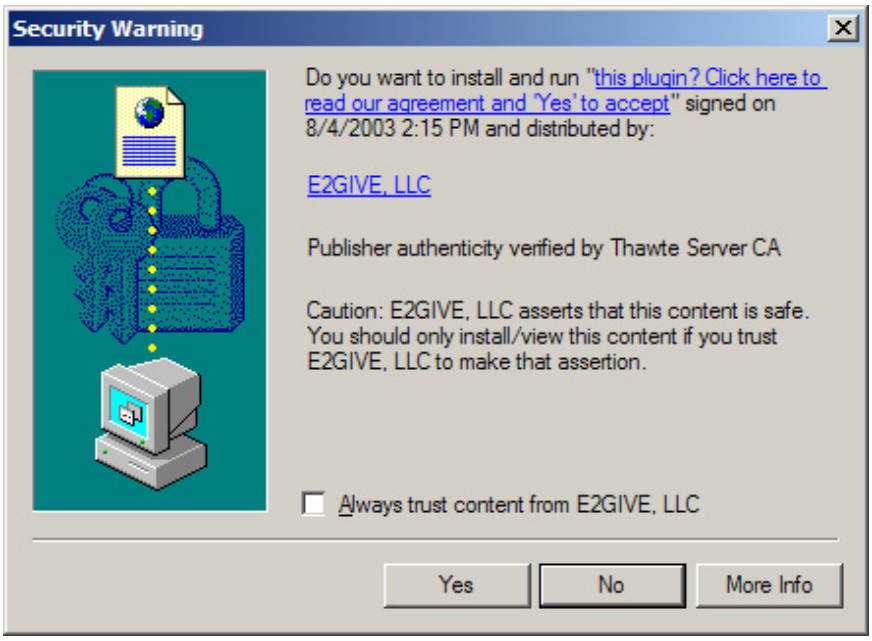
In my opinion, when a consumer downloads software represented as assisting with timekeeping and displaying calendar information (as is the case with PrecisionTime and Date Manager, respectively), it is highly unlikely that the consumer will expect that same software to secretly track their Web browsing habits and to generate pop-up advertisements. This is in some respects analogous to adhesion contracts which contain provisions so wildly disparate from that which a reasonable user might expect, that as a matter of public policy, courts regularly refuse to uphold the validity of such contracts. In my opinion, given that pop-up ad generation is the fundamental function of the GAIN ad-serving software, the choice to place the first mention of that functionality on the fourth page constitutes a "burying" of the notice.

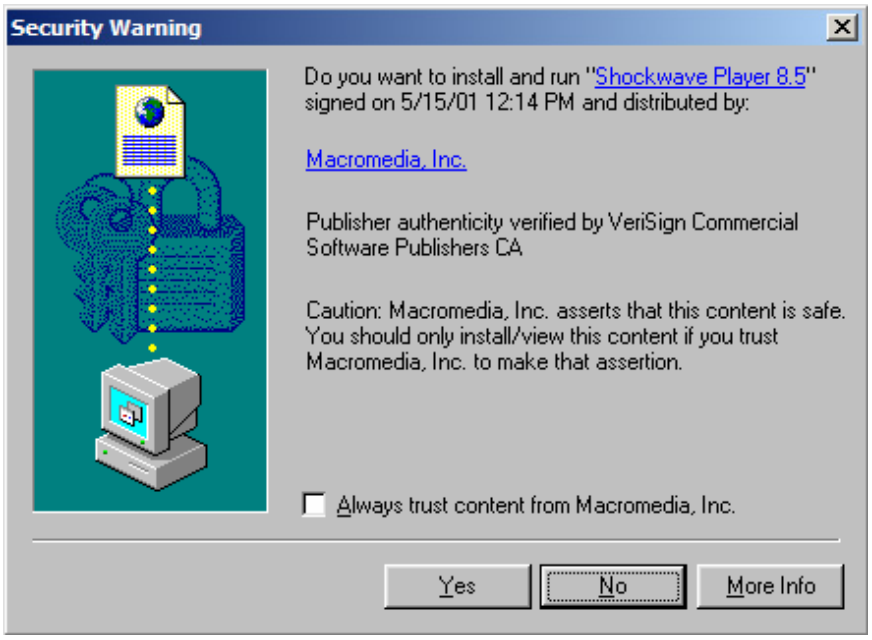
At this point, I should note that Claria is by no means unique among distributors of spyware in providing consumers with inadequate notice and choice. For example, I have found similarly uninformative installation disclosures in software distributed by E2Give, Xupiter, BetterInternet (the current incarnation of the VX2 software discussed above), and TotalVelocity. While many of these companies include disclaimers about their software buried in EULAs and lengthy privacy policies, it is my experience, and indeed common knowledge shared by many, that consumers seldom read the "fine print" when they are impatient to complete a transaction. That belief is further supported by the findings of a survey project conducted at Texas A&M University-Commerce, which found that 54.7% of the respondents in that survey do not read online privacy policies.[18]

TAKING ADVANTAGE OF CONSUMER INEXPERIENCE

In my opinion, I believe that many spyware companies also take advantage of consumer inexperience and naïveté regarding the processes by which software comes to be installed while those consumers surf the Web. For example, in researching *Internet Privacy for Dummies*, I discovered that the installation dialog box for many spyware applications is nearly identical to that of other popular software packages such as Quicktime, Real Networks' RealPlayer/RealOne, Macromedia's Shockwave and Flash plug-ins, and Adobe's Acrobat Reader software. Compare these two installation dialog boxes:

[18] Greg Blasingane, et. al., *Online Privacy: A United States Perspective*, http://boisdarc.tamu-commerce.edu/~bkusle/mkt/Internet_Privacy.pdf at 17 (visited January 21, 2004)





The installation boxes are for the E2Give spyware application and the popular and widely-used Macromedia's Shockwave software, which enables Web sites to offer dynamic interactive and multimedia features. Similar installation boxes arise when installing Quicktime and RealPlayer/RealOne, popular software used to display full motion video clips and music recordings. Macromedia also distributes a popular application called Flash, which displays interactive animations for Web site menus, games, and other content. The Commission is also familiar with Adobe's Acrobat Reader, software which permits the viewing and printing of complex desktop publishing documents, such as electronic versions of tax forms provided by the Internal Revenue Service, as well as many documents distributed by the Commission on its Web site.

While I do not profess expertise in the technical functions of all these applications, to the best of my knowledge, none of those software packages perform any tracking of a user's Web viewing activities for purposes of generating pop-up ads. Indeed, those software packages provide access to entirely new categories of dynamic multimedia content which cannot be viewed otherwise without the software installation process. In my opinion, those software packages and many others like them are a vital part of what makes the Internet more attractive to consumers, and for many companies such software plays a critical role in attracting consumers to their Web sites for purposes of e-commerce.

In my opinion, when users visit Web sites and, upon arriving, are asked to download a piece of software, the clear implication – which has been reinforced by repeated frequent consumer experience as evidenced by the remarkably high installation percentages for Adobe Acrobat[19] and Quicktime[20] – is that the software is necessary to view or interact with the website. It is my opinion that many spyware distributors take unfair advantage of that user behavior in order to get spyware installed on users' computers.

In my experience, the average user is conditioned to click "Yes" on all the dialog screens in order to get on with the business of viewing the content they requested. This experience was confirmed when, during the course of interviewing friends and acquaintances in preparation for writing my book, many of those questioned indicated that their past experiences with the benefits of installing such software packages had indeed made them accustomed to reflexively and immediately clicking "Yes" when presented with such dialog boxes. Thus, my co-authors and I devoted a portion of one chapter in our book to warning users that, while some software add-ons are completely innocuous, other software packages act as a "Trojan Horse," disguised as something pleasant but ultimately delivering an unsavory payload.

In my opinion, many spyware companies are fundamentally based on a Trojan Horse model, because many of the software packages being presented as "free" are done so with the hope that consumers do not notice that bundled inside that package is something more which delivers an unwanted surprise in the form of pop-up ads. In my opinion, spyware distributors take unfair advantage of the many millions of unsuspecting and unsophisticated Internet users who, as a result of past experiences with seeking entertaining Web site content, will uncritically accept such "gift" software downloads without fully understanding or appreciating the consequences of doing so.

SOWING SEEDS OF CONSUMER DISTRUST AND SUSPICION

Another negative impact of the proliferation of spyware in many "free" software applications is that consumers will increasingly grow to distrust such applications, hindering the growth and deployment of those new technologies. Many Web sites take advantage of the latest

[19] According to Adobe, makers of Acrobat, more than 500 million copies of the software have been distributed. http://www.adobe.com/products/acrobat/main.html (visited March 18, 2004)
[20] According to Apple Computer, makers of Quicktime, the latest version of their software was downloaded 175 million times in the first 18 months it was available. http://www.apple.com/quicktime/whyqt/ (visited March 18, 2004)

technologies for enhancing Web site users' experiences, such as music and full-motion video, intricate animations, and dynamic navigational controls. In many cases, consumers find that in order to utilize these cutting-edge features, they must download and install free software to add additional functionality to their Web browsing software. Based upon my interactions with many consumers who have unknowingly installed free software only to find their computer became infected with spyware, it is clear that many consumers become much more distrustful of these new technologies. It is my opinion that those negative reactions will inevitably translate into users associating Web-based "free" software downloads with practices such as unwanted pop-up ads.

Obstacles to deployment of new Web technologies will also have a significant impact upon one of the fastest growing areas of Internet advertising, known as "Rich Media" advertisements. Analysts indicate that Rich Media ads are one of the hottest areas of the online advertising market.[21] However, one obstacle to the growth in the usage of Rich Media advertisements is that many of them require additional software to be installed in order to run. For example, many of the Rich Media advertisements that I have experienced online require Macromedia's Flash software to be installed by the user in order to view the video, sound, and animations in the Rich Media advertisements. Advertisers are able to take advantage of the fact that many of these software packages are installed by users seeking to access other Rich Media content, such as online movies and games. However, when users reject these new technologies out of fear and uncertainty, advertisers are unable to deploy advertisements that take advantage of them.

As consumer frustration with spyware grows, and that anger becomes inevitably translated to distrust of unexpected software downloads, the deployment of these new technologies may be hindered by negative consumer attitudes. Web site operators will in turn respond to consumer fears by declining to make use of new technologies, many of which often require the user to download and install software in the same manner employed by so many of the spyware distributors. It is my conclusion, therefore, that as consumers develop negative attitudes toward free software downloads, those fears will have an adverse impact on the deployment of such new technologies and serve as an unwelcome drag on the market for new and innovative ways of presenting information to consumers.

THE CONTRAST WITH ADWARE

I believe it is important to contrast the functionality and behavior of spyware with the other topic of the Commission's inquiry: adware. I define adware as being a category of software for which the costs of development and distribution are subsidized by advertisements appearing as an integrated part of the software application. Generally speaking, I would identify the main difference between spyware and adware as being the relative transparency of the relationship between the software and the advertisements displayed as a direct result thereof.

[21] Brian Morrissey, *Beyond the Banner: Will Rich Media Win the Day?* InternetNews.com (October 23, 2003) at http://www.internetnews.com/IAR/article.php/1487071 (viewed on March 18, 2004)

For example, there are numerous examples of advertising-supported software which do not obscure the Web pages being visited and do not unfairly divert traffic in a manner that negates a Web site's investment in advertising and marketing. The popular email software application Eudora[22] offers a free, ad-supported version which presents advertisements in a panel appearing in the menu bar of the application. Similarly, the free version of the Web browsing software Opera[23] displays ad banners adjacent to the Web browser's navigational buttons. There is little possibility of confusion regarding the origins of the ads, and the application whose operation is being subsidized by those ads.

While it is possible for adware to have spyware characteristics, such as the gathering and transmission of user information without notice or choice to consumers, the presence of the advertising in a clear relationship to the operation of the software serves to give consumers some level of notice that something more is going on with the software.

SECURITY RISKS ARISING FROM SPYWARE

Inherent to the issue of spyware is the notion that there is software operating on a user's computer, often without their knowledge or consent. Just as with computer viruses and worms, the risks of having unauthorized software operating on one's computer can be quite significant. Surreptitiously installed software could be performing any number of tasks, from generating annoying pop-up ads, to installing additional pieces of software, to crashing the computer. Indeed, in the course of researching my book, I found that the first indication that many consumers have of spyware on their computer is degradation in system performance and unexplained system crashes.

Another problem arising from the presence of spyware on a computer is that it creates the possibility of additional security breaches on that computer. For example, many of the spyware applications of which I am aware have functions that allow them to take control of a computer's Internet connection to communicate with the software's creator. Not only is it possible for private and personal information to be transmitted over that connection, but the connection itself represents a potential security risk. One of the most critical elements of computer security is to limit the ways in which a computer may be connected to other computers. Unknown connections to a user's computer via unauthorized backchannels pose a significant risk.

In one particularly concerning case, a colleague of mine was contacted by a major corporation in a regulated industry regarding privacy and security issues involving spyware. As we learned, they had recently deployed an online educational tool throughout their organization. In distributing the software, one component included the DIVX digital video Codec which contained a spyware application. Unbeknownst to the company, the spyware was now installed on tens of thousands of computers worldwide, including many workstations where sensitive financial information of consumers was processed. Due to the surreptitious manner in which many types of spyware monitors activities in Web browsing software, coupled with the company's deployment of various internal Web-based tools for accessing and processing

[22] See http://www.eudora.com/download (visited March 18, 2004)
[23] See http://www.opera.com/advertise (visited March 18, 2004)

sensitive financial information, it is possible that data from private financial records could have been inadvertently transmitted to the spyware firm or its advertising partners.

THE SPECIAL PROBLEM OF KEYSTROKE LOGGERS

Perhaps the greatest risk to consumers is the surreptitious installation of the most comprehensive form of spyware, a "keystroke logger." Much as the name implies, a keystroke logging program creates a record of every key pressed by a computer's user, and sends that data back to the creator of the spyware. By tracking every piece of information entered by a consumer, it is easy to learn their interests and preferences for marketing purposes. But it is also a trivial matter to record every piece of financial or health information they enter into the computer, every password and identity code they use to access private information inside any application, and every message they type to friends, family, or coworkers. In short, keystroke loggers create a perfect word-for-word record of everything a user does on their computer, allowing a third party to eavesdrop on their most private and intimate information.

CONCLUSIONS

In conclusion, it is my opinion that, contrary to the claims of many spyware distributors, spyware creates a myriad of harms and risks to consumers and to the competitive environment. The harms to consumers include the deceptive practices that often accompany the distribution and installation of spyware, and the fear and suspicion bred in consumers as they later learn the manner in which they've been taken advantage of. Arising from that consumer fear, spyware creates harms that risk affecting the growth and deployment of new technologies, many of which are intended to improve the consumer experience. When taken together, I believe all of these circumstances suggest that spyware constitutes exactly the kind of unfair and anti-competitive practices that the Commission was created to protect against. I urge the Commission to act decisively to prevent the proliferation of spyware and their attendant harms.

Respectfully submitted,

/s/

Ray Everett-Church