UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re SONY BMG CD TECHNOLOGIES LITIGATION	:	Civil Action No. 1:05-cv-09575-NRB
	:	CLASS ACTION
This Document Relates To: ALL ACTIONS.	:	DECLARATION OF LARRY PONEMON IN SUPPORT OF THE RICCIUTI CLASS REPRESENTATIVES' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR AN AWARD OF ATTORNEYS' FEES AND REIMBURSEMENT OF EXPENSES

EXHIBIT B

Presents

National Spyware Study©

Conducted by Ponemon Institute, LLC

Report Issued May 17, 2005

National Spyware Survey

Summary Report Prepared by Dr. Larry Ponemon, May 17, 2005

Sponsor: Unisys Corporation, Security Leadership Institute.

An overwhelming number of adult-aged Internet users believe they have had their computers infected with spyware. Some report that in the past 12 months spyware-related problems have cost them approximately $50. If this cost is extrapolated to the entire population of Internet users, the total monetary loss could reach hundreds of millions every year.

Despite the cost and other problems experienced as a result of spyware, a majority of Internet users in this study don't want any new anti-spyware laws passed that would prevent them from downloading free software such as music players, games or screen savers.

Sponsored by Unisys Corporation, the 2005 National Spyware Survey was conducted by Ponemon Institute to learn what consumers know about spyware, how they believe spyware differs from adware or researchware, how spyware has affected their computers and what they think should be done to curtail this problem.

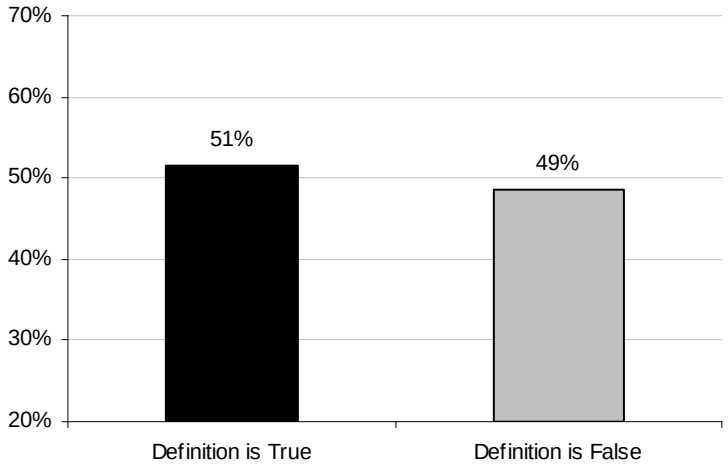
The Web-based survey was distributed to over 15,000 individuals who self-reported that they have a dedicated laptop or desktop computer to spend at least one hour each day on the Internet. In total, we received 1,944 usable responses. Please note that caution should be applied when extrapolating sample results to the general population because of this specialized subject pool.

Internet Users Are Confused

An important finding from our research is that consumers have a hard time distinguishing spyware from adware. As shown in Bar Chart 1, the survey asked respondents to indicate whether they believed that the following statement is true or false.

"Both spyware and adware assist in gathering information about a person or organization and sends it to other interested parties. The difference is that you agree to download adware in exchange for free software or other offers. Spyware is downloaded without your consent or awareness that it is on your computer collecting information about you."

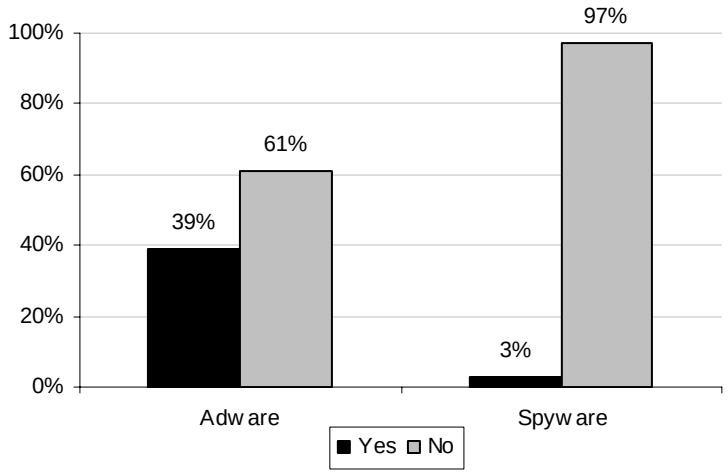
Bar Chart 1: Is the definition of spyware and adware correct?



The above definition is considered correct; thus, a high false response suggests that respondents failed to understand the basic differences between spyware and adware. As shown, 49% of survey respondents believe the definition in the survey is not correct.

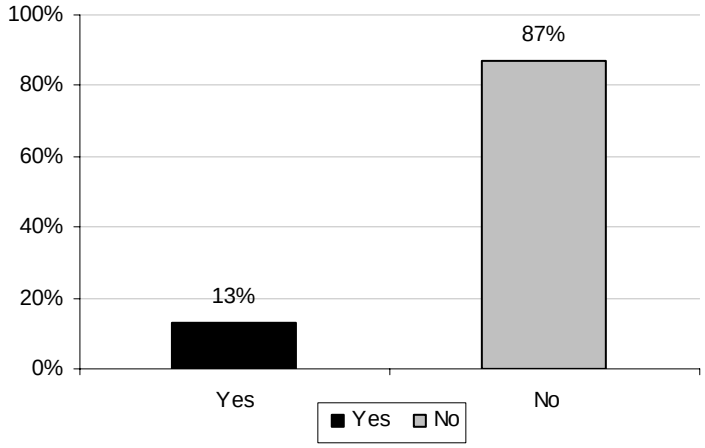
More than 84% of respondents believe they are victims of spyware and more than 42% admit to having "no idea" where it came from. Further, 61% did not recall giving their permission to download adware and 97% did not recall giving permission to download spyware onto their primary computer. See Bar Chart 2.

Bar Chart 2: Do you remember giving permission to download adware or spyware?



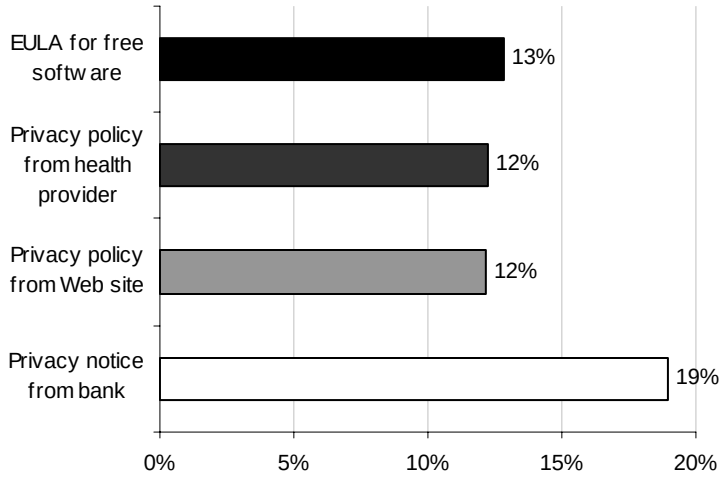
It is interesting to note that when available most individuals admit that they do not read EULAs because the language in the EULA is too complex and confusing. See Bar Chart 3.

Bar Chart 3: Do you read the EULA before downloading free software?



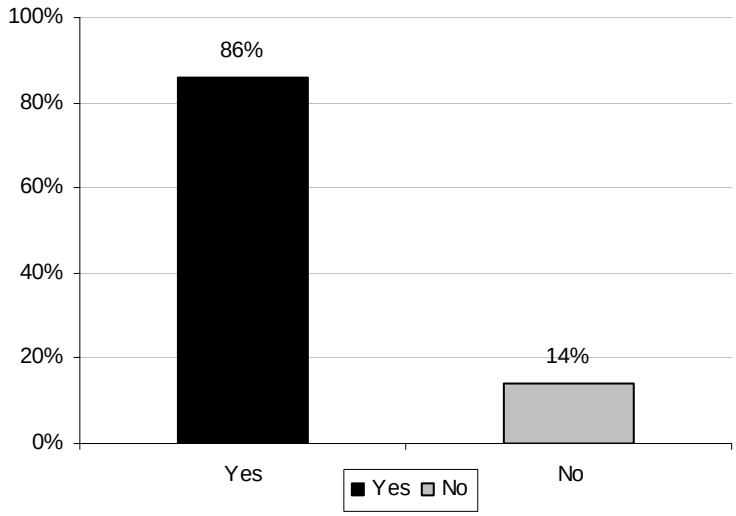
Bar Chart 4 provides a side-by-side comparison of respondent's self-reporting reading preferences for bank privacy notices, Web privacy policies, health care provider privacy policies and EULAs. It shows that the percentage of those who do not read the EULA is comparable to the percentages for not reading privacy notices and Web policies.

Bar Chart 4: Comparison of EULA to other privacy-related policies



Bar Chart 5 provides the percentage of self-reported spyware victims who experience (yes) or did not experience (no) a monetary loss, productivity loss or serious inconvenience as a result of the spyware infection.

Bar Chart 5: Spyware victims who report experiencing a monetary or productivity loss



Our results suggest that a majority of respondents do not understand the ad serving marketplace. Accordingly, they do not know how "free" software programs earn profits for their suppliers. In addition, they seem to want their cake and eat it too. Respondents believe free software should be given with no strings attached such as the ability of the company to profile or track online activities. For example, 48% reported that it is never acceptable to track their Internet activities.

Survey

As part of the survey instrument review process, we sought input from a number of learned sources including privacy advocates, ad software technologists and other experts.

The survey utilized a fixed cluster sampling frame. The target respondents were recruited based on self-reported demographic criteria including familiarity with the Internet. Subjects were invited to participate by e-mail.

Respondents were given the following basic instructions before starting the survey process.

Dear Respondent:

We would like to learn what you think about software known as spyware and adware that is downloaded onto computers. Please take about 15 minutes to respond to the survey.

Please refer your answers to the computer desktop or laptop that you most frequently use for personal activities such as browsing the Internet.

All responses will remain completely confidential and no personally identifiable information will be collected. Thank you for your prompt response.

Items on the survey form were randomized or rotated to mitigate order effects. All completed returns were evaluated for consistency and internal reliability before including in our database.

Sample

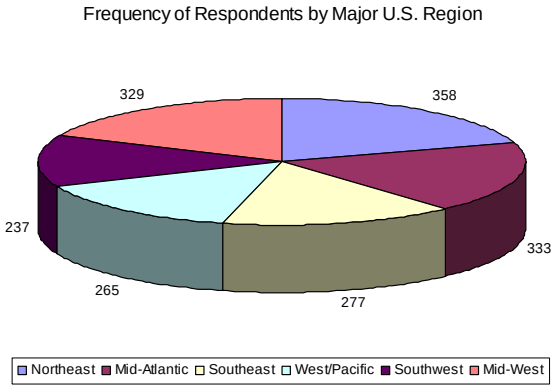
Following are the response statistics and geographic distribution across the United States. In total, 2,218 adult-aged Internet users submitted survey results. Of these responses, 274 (1.8%) were deemed to be inconsistent or unreliable. This resulted in 1,944 usable surveys.

Our final sample represents 12.6% of the sampling frame. Please note that this response rate is lower than earlier Web-based studies completed by us. This is most likely due to a shorter than normal holdout period. Our survey field work was captured within 10 days. Non-response bias is currently being investigated and will be reported in a future report.

The following Pie Chart shows that the two most heavily represented regions include the Northeast and Mid-Atlantic regions of the United States.

Sample Characteristics	Total	Pct %
Sample frame	15413	100.0%
Total responses	2218	14.4%
Total rejections	274	1.8%
Net responses	1944	12.6%

Geographic regions	Freq	Pct%
Northeast	386	20%
Mid-Atlantic	374	19%
Southeast	301	15%
West/Pacific	299	15%
Southwest	256	13%
Mid-West	328	17%
Total	1944	100%



As noted before, our sampling frame is a subset of a larger set of clusters. By design, our sample represented those adults who: (1) owned or had control over their own computer (desktop or laptop) and (2) used the Internet one or more hour each day. Hence, care needs be taken when trying to generalize and apply these findings to all Internet users in the United States.

Detailed Findings

The actual survey frequencies and percentage frequencies are reported in tabular format. Following are the two control questions about the operating system and Internet browsers of the respondent's primary computer.

Q1. What is your computer's operating system that you use most of the time for Internet browsing or shopping activities?	Freq	Pct%
Microsoft Windows	1,777	91%
Others	167	9%
Total	1944	100%

Q2. What is the browser that you typically use to access the Internet?	Freq	Pct%
Internet Explorer	1,746	90%
Netscape	73	4%
Firefox	71	4%
Others	54	3%
Total	1,944	100%

A majority (57%) of respondents state that they do not share primary computer with family members or friends.

Q3. Do you share your computer with others, such as family members or friends?	Freq	Pct%
Yes	841	43%
No	1,103	57%
Total	1,944	100%

The following question served as a test of respondents' understanding of the main differences between spyware and adware. Because the definition provided within our instrument is generally considered correct by learned sources, a high false response indicates that respondents fail to understand the basic issues and nuances of spyware versus adware. As shown, 49% believe that this definition is false.

Q4. Both spyware and adware assist in gathering information about a person or organization and send it to other interested parties. The difference is that you agree to download adware in exchange for free software or other offers. Spyware is downloaded without your consent or awareness that it is on your computer collecting information about you.	Freq	Pct%
I believe the above definition is true	1000	51%
I believe the above definition is false	943	49%
Total	1943	100%

The following two questions assess the respondents' understanding of ad delivery from cookies and adware downloads.

Q5A. Are you aware if the Internet or software on your computer sends you ads such as pop-ups or banners?	Freq	Pct%
Yes	1713	88%
No	231	12%
Total	1944	100%

Q5B. Are you aware if ad software on your computer sends you ads such as pop-ups or banners?	Freq	Pct%
Yes	881	45%
No	1061	55%
Total	1942	100%

Questions 6 A to D were completed by those respondents stating Yes in the above item.

The next question shows that many subjects do not understand what adware does.

Q6A. What does this adware do? Please check only one response.	Freq	Pct%
I have no idea what this software does.	492	56%
The software captures personal information.	111	13%
The software captures information about my online activities.	203	23%
The software captures information from my emails and other stored documents	74	8%
Total	880	100%

The following question shows that many respondents do not recall giving permission to the adware company prior to downloading desktop software.

Q6B. Do you recall giving permission to have this ad software downloaded onto your computer?	Freq	Pct%
Yes	345	39%
No	536	61%
Total	881	100%

The next question shows that many respondents believe that adware negatively affects their computer's performance or reliability (as indicated by Yes or Unsure response).

Q6C. Does this ad software negatively affect your computer's performance or reliability?	Freq	Pct%
Yes	321	37%
Unsure	288	33%
No	270	31%
Total	879	100%

The following question shows how respondents define the performance or reliability problems inherent in adware. Over 88% of these subjects believe that adware slows down their computer performance. Over 31% believe that adware collects data from stored files such as e-mails and documents.

Q6D. Please check those issues that you experienced as a result of ad software.	Freq	Tot%
It slows down my computer.	534	88%
It modifies certain computer or browser settings.	133	22%
It turns off certain computer security settings.	158	26%
It collects emails, records and files on my computer's storage devices.	186	31%
It hijacks my computer, directing it to perform activities outside of my control.	45	7%

Over 90% of respondents report that they download free software from the Internet.

Q7A. Have you ever downloaded free software from the Internet?	Freq	Pct%
Yes	1745	90%
No	197	10%
Total	1,942	100%

Following is the distribution of software most likely to be downloaded on the Internet for free. Notice that music file sharing programs are the most commonly downloaded free software programs. Games and screen savers are also popular.

Q7B. What type of free software was it (please check all that apply)?	Freq	Tot%
Screen saver	755	43%
Music file sharing such as Napster, Morpheus, and Grokster	1056	61%
Anti-spam or pop-up blocker	354	20%
Games	977	56%
Search toolbar	347	20%
Ring tones on cellular phone	128	7%
Free telephone or VoIP service	78	4%
Spyware removal tool	319	18%
Web accelerator	244	14%

The next question shows that 87% of subjects admit that they <u>do not</u> read the EULA prior to loading free software.

Q7C. Before you download free software programs from the Internet, do you generally read the legal terminology presented to you prior to the download (also known as the End User License Agreement or EULA)?	Freq	Pct%
Yes (proceed to Q8)	251	13%
No	1693	87%
Total	1,944	100%

The following question attempts to assess why respondents don't read the EULA. As can be seen, the two most common reasons are that the document is too long and too complex.

Q7D. Why don't you read the EULA?	Freq	Tot%
It takes too long to read the EULA.	1488	88%
The EULA language is too complicated or is difficult to understand.	1314	78%
I trust the software company so it is not necessary to read the agreement.	115	7%
I can get the information directly from the software after downloading it.	203	12%

The next question tries to ascertain what Internet software and ad marketing companies can do to encourage a higher reading rate among those downloading free products. Respondents suggest that the best way to improve readability is to make the EULA shorter and place it on one Web page or screen that does not require a scrolling option.

Q7E. What could be done to encourage you to read the EULA before downloading free software (please check all that apply)?	Freq	Tot%
Make the EULA easier to read.	1213	72%
Place a shorter EULA on one screen rather than having to click to a separate document and then scroll down.	1108	65%
Require the EULA to be printed prior to allowing the free software from downloading.	513	30%
Provide EULA highlights that provide warning about serious risks to you.	607	36%
Nothing can be done that will cause me to read the EULA.	455	27%

The following question provides the respondents' opinion to key statements concerning adware, spyware and free software. A lower average rank suggests that subjects tend to agree with the statement. A higher average rank implies disagreement with the statement.

Q8. Place a number 1 to 5 next to each statement that best indicates your opinion about the statement presented below. Please use the following 1 to 5 scale to define your opinion about statements in Q8 and Q9.	Average Rank	Order
I like having the ability to obtain free software on the Internet.	2.03	1
I like having access to free search engines on the Internet.	2.36	2
I don't mind ad software on my computer if it does not collect information that identifies me or my family.	3.59	5
I don't mind ad software on my computer even if it collects information that identifies me or my family.	4.34	7
I don't mind ad software on my computer as long as I'm given advance warning or notice before I download free software on the Internet.	3.07	4
I generally expect to get ad software on my computer every time I download a free software product from the Internet.	2.43	3
I would be willing to pay a small price or fee for software that I received for free, as long as this guarantees that I don't get ad software as part of the download.	3.64	6

As shown above, subjects like to obtain "free software" online (average rank=2.03). They don't want to pay, even a small amount, to prevent adware or spyware. Respondents do not want adware to collect information that identifies them and their families (average rank=4.34).

The following question provides the respondents' opinion to key statements concerning the need for new regulations about spyware. As indicated by an average rank of 2.20, respondents do not want anti-spyware regulations that limit their ability to get free software on the Internet. They are uncertain (average rank of 3.06) about the need for new laws to regulate the Internet.

Q9. What do you think about government regulations that protect consumers from spyware? Please place a number 1 to 5 next to each statement that best indicates what you think.	Average Rank	Order
There is a need for a new law to prevent spyware from downloading onto my computer, even if it prevents me from obtaining free software.	2.67	2
There is a need for a new law to prevent adware from downloading onto my computer, even if it prevents me from obtaining free software.	3.32	4
There is no need for additional laws that regulate the Internet.	3.06	3
New anti-spyware laws should not prevent me from downloading free software.	2.20	1

The next question provides a relative comparison of the respondents' reading preferences for a EULA in relation to three commonly encountered privacy policies. As shown, while a majority of respondents admit to not reading the EULA, they also don't read privacy notices or Web policies.

Q10. Place a 1=True or 2=False next to each statement to best indicate or reading preference.	True	Pct%
I usually read the privacy notice provided by my bank or other financial service companies.	369	19%
I usually read the privacy policy posted on my favorite Web sites.	236	12%
I usually read the privacy policy provided by my health care provider or physician.	238	12%
I usually read the end user license agreements (EULA) provided by a software company.	249	13%

The following item attempts to assess respondents' understanding of Internet economics specifically regarding how free software companies earn a profit.

Q11. How do companies that download free software over the Internet earn enough revenues to stay in business? Please check what you believe to be best choice.	Freq	Pct%
The free software company obtains a commission from the ad software company for each successful download.	348	18%
The free software company asks you to purchase upgrades or related products.	312	16%
The free software company charges a fee from end-users after a trial period.	341	18%
The software companies receive voluntary donations from end-users.	58	3%
I have no idea.	881	45%
Total	1940	100%

As noted above, over 45% admit that they do not have any idea whatsoever. The pattern of responses to Q11 suggests that subjects do not have a clear understanding of the Internet or ad serving marketplace.

The next item ask respondents' to state their belief regarding the role that anti-virus software or pop-up blockers play in protecting them from spyware. Responses suggest that subjects do not hold a consistent view about how these solutions resolve the spyware problem.

Q12. Do you believe that anti-virus software or pop-up blockers will protect you from spyware?	Freq	Pct%
Yes	893	46%
No	1048	54%
Total	1941	100%

The following question asks respondents to state their beliefs about being tracked when browsing the Internet. Over 62% of subjects believe that they are tracked.

Q13A. Do you believe Internet advertisers, publishers and other content providers currently track your activities and movement across the Internet?	Freq	Pct%
Yes	1201	62%
No	739	38%
Total	1940	100%

The following table shows that 48% of subjects believe that it is never acceptable to have their activities tracked on the Internet.

Q13B. When is it acceptable to track your activities and movement across the Internet?	Freq	Tot%
To perform research that improves a company's products or services.	519	43%
To conduct surveillance for national security purposes.	454	38%
To send ads that provide offers that you might find interesting or relevant.	442	37%
To provide information or content that fits your interests, tastes and preferences.	501	42%
It is never acceptable to track my activities on the Internet.	579	48%

The next several items report the respondents' experiences with spyware. As shown, over 84% of respondents believe that they have been the victim of spyware on their computer.

Q14A. Has your computer ever been infected with spyware?	Freq	Pct%
Yes	1630	84%
No	309	16%
Total	1939	100%

With respect to spyware victims, over 97% do not recall giving their permission to download software onto their computer.

Q14B. Do you recall giving permission to download the spyware software on your computer?	Freq	Pct%
Yes	56	3%
No	1572	97%
Total	1628	100%

The next table shows that over 42% of subjects have no clue as to how spyware was downloaded onto their computer. Another 38% believe that this was the consequence of a free software download.

Q14C. How did your computer become infected with spyware?	Freq	Pct%
A friend or family member was using my computer.	85	5%
I downloaded free software.	621	38%
It downloaded automatically when I visited a particular Web site.	134	8%
It was already loaded when I bought my computer.	107	7%
I have no idea.	682	42%
Total	1629	100%

Over 43% of subjects became aware of spyware through security software alerts or anti-spyware software. Over 32% of respondents just had a gut feel or instinct that their computer was infected with this illegal software.

Q14D. How did you find out that you had spyware on your computer?	Freq	Pct%
Warning from anti-virus or anti-spyware software	706	43%
A computer expert told me	157	10%
I just knew based on my computer's performance or reliability	520	32%
Unsure	246	15%
Total	1629	100%

About 35% of subjects state that they could not remove the spyware. Another 22% stated that they used an anti-spyware (or security software tool) to remove this illegal software. Only 21% state that they used un-install utilities to remove the spyware from their computer system.

Q14E. How did you remove the spyware on your computer?	Freq	Pct%
I uninstalled the software	341	21%
I used anti-spyware software	354	22%
I hired a computer expert	154	9%
I could not remove the spyware software	568	35%
I did not try to remove the spyware software	211	13%
Total	1628	100%

For those who performed a un-install procedure to get rid of the spyware from their computer system, over 36% report that this was not difficult to do.

Q14F. How difficult was the un-installing task for you?	Freq	Pct%
Very difficult	51	15%
Difficult	67	20%
Moderately difficult	86	25%
Not difficult	123	36%
Easy	13	4%
Total	340	100%

The next items attempt to determine the approximate monetary loss and productivity (time) loss resulting from spyware over the past 12 months. As shown, over 86% of those who report having been infected with spyware believe they have experienced a monetary loss, a productivity loss or some other inconveniences.

Q15A. Has spyware on your desktop or laptop caused you to suffer a monetary loss, a productivity loss or inconvenience?	Freq	Pct%
Yes	1401	86%
No	229	14%
Total	1630	100%

The following table shows that the most common form of loss resulting from spyware infection is a decline in productivity (as reported by about 87% of respondents). Over 26% of subjects stated that they purchased security solutions to respond to spyware threats. Another 14% stated that they hired computer consultants to repair system.

Q15B. What best describes this negative impact (check all that applies)?	Freq	Pct%
Purchased anti-spyware or anti-virus software.	371	26%
Hired a computer pro to fix my desktop or laptop.	200	14%
Replaced my computer with new hardware.	28	2%
Could not use previously downloaded software.	475	34%
Experienced productivity losses.	1214	87%
Purchased additional protection services from my ISP or DSL provider.	128	9%
Leakage of my personal information without consent or knowledge.	51	4%
Monetary damages resulting from criminal activity.	10	1%

The next question shows that about 85% of respondents did not experience any monetary (out of pocket) losses resulting from spyware infection. On average, for the 205 subjects (15%) in this study who did experience a monetary loss, the average amount of the loss is $49.70 (based on extrapolation from the table below) over the past 12 month period.

Q15C. Approximately, what is the monetary or out-of-pocket loss over the past 12 months as a result of having spyware on your computer? Please check the range that is closet to the total loss experienced.	Freq	Pct%	Average Cost	Ext Cost
No Monetary Loss	1190	85%	-	-
Between $0 and $10	23	2%	5	115
Between $10 and $20	66	5%	15	990
Between $20 and $50	60	4%	35	2,100
Between $50 and $100	31	2%	75	2,325
Between $100 and $200	12	1%	150	1,800
Over $200	13	1%	220	2,860
Total	1395	100%	Average	$49.7
Number of people with self-reported monetary loss	205	15%		

The next question shows that the vast majority of respondents report that they spent time to deal with their spyware infection. For the 1,066 subjects (76%) who reported some time loss, the average amount of time spent is approximately 1.6 hours per person over the past 12 month period.

Q15D. Approximately, how much time did you spend over the past 12 months as a result of having to deal with spyware on your computer? Please check the range that is closet to the total time spent by you.	Freq	Pct%	Avg Time	Ext Time
No time	336	24%	-	-
Between 0 and 60 minutes	899	64%	1	450
Between 1 to 5 hours	123	9%	3	308
Between 5 to 10 hours	19	1%	8	143
Between 10 to 50 hours	15	1%	30	450
Between 50 to 100 hours	7	0%	75	525
Over 100 hours	3	0%	120	360
Total	1402	100%	Average	1.6 Hrs
Number of people who self-reported time loss	1066	76%		

Recommendations

As we have noted, the respondents in our study spend a significant time on the Internet. Despite their experience, 56% of respondents have no idea what adware does and only 23% believe that it captures information about their online activities. This confusion is further exacerbated by the existence of "bad apples" populating the ad network space.

Privacy advocate groups, government and politicians are very interested in this issue. However, the solution to the spyware problem might not be in new laws. Instead companies in the ad network space should consider becoming proactive in helping consumers gain more control over their online experience. This can include obtaining consumers' affirmative consent to the collection and use of their data, giving consumers clear and conspicuous notice about the network's collection and use of consumers' information and making the privacy policy and EULA easy to find, read and understand.

In addition to controls over "bad apples," our results suggest the need for consumer outreach to raise awareness and understanding about the risks associated with "free" software.

Ponemon Institute, LLC

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email:

Ponemon Institute, LLC
Attn: Research Department
212 River Street
Elk Rapids, Michigan 49629
231.599.2920
research@ponemon.org

EXHIBIT A

About Dr. Larry Ponemon

Dr. Lawrence A. Ponemon is the Chairman and Founder of the Ponemon Institute, a research "think tank" dedicated to advancing privacy and data protection practices. Dr. Ponemon is considered a pioneer in privacy auditing and the Responsible Information Management or RIM framework.

Ponemon Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a various industries. In addition to Institute activities, Dr. Ponemon is an adjunct professor for information ethics and privacy at Carnegie Mellon University's CIO Institute and is faculty of CyLab. He serves on the Unisys Corporation's Security Leadership Institute Board and the IBM Privacy Management Council.

Dr. Ponemon is a member of the National Board of Advisors of the Eller College of Business and Public Administration, University of Arizona. He serves on the Government Policy Advisory Committee and Co-Chair of the Internet Task Force for the Council of American Survey and Research Organizations (CASRO).

Dr. Ponemon consults with leading multinational organizations on global privacy management programs. He has extensive knowledge of regulatory frameworks for managing privacy and data security including financial services, health care, pharmaceutical, telecom and Internet. Dr. Ponemon was appointed to the Advisory Committee for Privacy for the United States Federal Trade Commission. He was also an appointed to two California State task forces on privacy and data security laws. Dr. Ponemon currently serves as a privacy advisor to the United States Transportation Security Administration and Department of Homeland Security.

Dr. Ponemon was a senior partner of PricewaterhouseCoopers (where he founded the firm's global compliance risk management group). Prior to joining Price Waterhouse as a partner, Dr. Ponemon served as the National Director of Business Ethics Services for KPMG Peat Marwick, and was appointed Executive Director of the KPMG Business Ethics Institute.

Dr. Ponemon has held chaired (tenured) faculty positions at Babson College, Bentley College and SUNY Binghamton. He published numerous articles and learned books. He has presented more than 500 keynote speeches or learned presentations at national or international conferences on privacy, data protection, information security, corporate governance, and responsible information management. Dr. Ponemon is an active member of the International Association of Privacy Professionals, serving as founding member of the Certified Information Privacy Professional (CIPP) Advisory Board.

Dr. Ponemon is column editor for Computerworld, CSO Magazine, CMO Magazine, BNA and other leading publications. He is a frequent commentator on privacy and business ethics for CNN, Fox News, CBS, CNBC, MSNBC, The Wall Street Journal, New York Times, Washington Post, USA Today, Financial Times, Business 2.0, Newsweek, Business Week, U.S. News & World Report, CIO Magazine, Industry Standard, Boston Globe, InfoWorld, InformationWeek, Forbes, Fortune, CFO Magazine, Red Herring, Dow Jones News and others.

Dr. Ponemon earned his Ph.D. at Union College in Schenectady, New York. He has a Master's degree from Harvard University, Cambridge, Massachusetts, and attended the doctoral program in system sciences at Carnegie Mellon University, Pittsburgh, Pennsylvania. Dr. Ponemon earned his Bachelors with Highest Distinction from the University of Arizona, Tucson, Arizona. He is a Certified Public Accountant (active license in Texas).

Dr. Ponemon is married and has two sons. He is a U.S. Navy, Vietnam War era veteran, receiving an honorable discharge.

I, LARRY PONEMON, declare as follows:

1. I am the chairman and founder of Ponemon Institute, a "think tank" dedicated to advancing responsible information and privacy management practices in business and government. The Ponemon Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations. Attached hereto as Exhibit A is a true and correct copy of my résumé. I have personal knowledge of the matters stated herein and, if called upon, I could and would competently testify thereto.

2. I am considered a leading international expert on privacy auditing and responsible information management. I have extensive experience in auditing self-regulatory frameworks for data protection and privacy compliance in the United States, Canada, the European Union, Hong Kong and other nations.

3. I was appointed to the Advisory Committee on online privacy and security by the United States Federal Trade Commission. I also serve on various state privacy commissions including the California State Privacy Task Force and other initiatives.

4. I was asked to provide an estimate of the potential cost impact that Web-users may have experienced as a result of Sony BMG's download of digital rights management (DRM) software products known as XCP or Media Max 5.0.[1] For purposes of my analysis, these two software technologies are referred to as spyware because the Web-user was unlikely to know, control or uninstall these software products, and they create the opportunity for the user's desktop or laptop computer to suffer malfunctions including security threats.

---

[1] MediaMax 3.0 was omitted from my analysis because this DRM software product does not appear to open a door to potential malfunctions or security threats.

5. My analysis of the spyware cost impact for consumers is based on sample research findings from a national study released in May 2005.[2] Research methods in this study utilized a survey instrument. Adult-aged individuals throughout the United States provided information about their spyware experience.

6. One set of survey questions dealt with the monetary cost and time-related effort associated with respondents' spyware experience. The research did not attempt to collect proof of expenses or other pieces of evidence concerning each individual's time-related efforts. All responses were self-reported within the survey instrument.

7. I believe that there are inherent limitations to survey research that need to be carefully considered before drawing inferences from sample findings to the present case. The following items are specific limitations that are germane to most perception-capture surveys:

(a) Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying experience or beliefs than those who completed the instrument.

(b) Sampling bias: Because sampling frames were derived from mail lists, the quality of results is influenced by the accuracy of contact information and the degree to which the list is representative of individuals who are informed about current events. We also acknowledge that the results may be biased by media coverage at the time of the study.

---

[2] National Spyware Study, Ponemon Institute Report, May 17, 2005. A true and correct copy of this study is attached hereto as Exhibit B.

(c) Self-report bias: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that subjects did not adequately describe their beliefs or perceptions regarding spyware.

8. The sample of results reference 1,630 respondents – all of whom indicating that they experienced some form of spyware infection (including adware and malware) on their computer sometime over a 12 month time period.[3]

Has spyware on your desktop or laptop caused you to suffer a monetary loss, a productivity loss or inconvenience?	Frequency	Total Percentage
Yes	1,401	86%
No	229	14%
Total	1,630	100%

9. The analysis shows that 1,401 respondents (86%) stated that spyware has caused them to suffer a monetary loss, a productivity loss or inconvenience. A second analysis required these 1,401 respondents to list their nature of negative experiences.

10. The following table provides a distribution of responses in ascending order of importance based on the frequency of responses. Please note that the percentage of total responses sums to more than 100% because respondents could check more that one item. The largest negative impact (87%) concerns the respondents' lost productivity as a result of spyware infection. The second most significant impact (34%) concerns respondents' inability to use previously downloaded software as a result of spyware infection.

---

[3] In this study, 87% of respondents said that they ***do not read*** the End User License Agreement or EULA prior to downloading software.

What best describes this negative impact? (Check all that apply.)	Frequency	Total Percentage
Experienced productivity losses.	1,214	87%
Could not use previously downloaded software.	475	34%
Purchased anti-spyware or anti-virus software.	371	26%
Hired a computer pro to fix my desktop or laptop.	200	14%
Purchased additional protection services from my ISP or DSL provider.	128	9%
Leakage of my personal information without consent or knowledge.	51	4%
Replaced my computer with new hardware.	28	2%
Monetary damages resulting from criminal activity or related abuses.	10	1%

11. The third analysis asked respondents to state an approximate monetary or out-of-pocket cost impact incurred over the past year. They were also given an opportunity to state "no monetary loss." In total, 205 respondents (15%) report a monetary loss as a result of spyware. The remaining 1,190 (85%) did not report a monetary loss.

12. For the 205 respondents who report a monetary loss, I extrapolated an average cost burden based on the median value for each one of six cost categories in the instrument (shown below).

13. For the highest cost category (over $200), I utilized a conservative median value of $220 (or 110% the category minimum).

Approximately, what is the monetary or out-of-pocket loss over the past 12 months as a result of having spyware on your computer? Please check the range that is closet to the total loss experienced.	Frequency	Total Percentage	Median Cost in Range	Calculation
No Monetary Loss	1,190	85%	-	-
Between $0 and $10	23	2%	5	0.1
Between $10 and $20	66	5%	15	0.7
Between $20 and $50	60	4%	35	1.5
Between $50 and $100	31	2%	75	1.7
Between $100 and $200	12	1%	50	1.3
Over $200	13	1%	220	2.1
Total	1,395	100%	Average	7.3
Number of people with self-reported monetary loss	205	15%		

14. The summation of all median values multiplied by the percentage frequency of responses in each cost category is the basis of a $7.3 point estimate for an overall monetary cost impact. This extrapolated cost burden is a value that applies to all 1,395 respondents, and not just those 205 people (15%) that reported a monetary loss. Hence, the extrapolated per capital cost is $1.07 (defined as $7.3 multiplied by 15%).

15. The fourth analysis asked respondents to state an approximate time impact incurred over the past year. They were also given an opportunity to state "no time" loss. A total of 1,066 respondents (76%) report time losses as a result of spyware. The remaining 336 (24%) did not report a time loss.

16. For the 1,066 respondents who report a time loss, we extrapolate an average time burden based on the median value for each one of six time range categories in the instrument (shown below). For the highest time category (over 100 hours), we utilized a conservative median value of 120 hours (or 120% the category minimum).

Approximately, how much time did you spend over the past 12 months as a result of having to deal with spyware on your computer? Please check the range that is closet to the total time spent by you.	Frequency	Percentage	Average Time Percentage	Calculation
No time	336	24.0%	-	-
Between 0 and 60 minutes	899	64.1%	0.5	0.32
Between 1 to 5 hours	123	8.8%	2.5	0.22
Between 5 to 10 hours	19	1.4%	7.5	0.10
Between 10 to 50 hours	15	1.1%	30.0	0.32
Between 50 to 100 hours	7	0.5%	75.0	0.37
Over 100 hours	3	0.2%	120.0	0.26
Total	1,402	100.0%	Average	1.59
Number of people who self-reported time loss	1,066	76.0%		

17. The summation of all median values multiplied by the percentage frequency of responses in each time category is the basis of a 1.59 hour point estimate for an overall time impact. This extrapolated time burden is a value that applies to all 1,402 respondents, and not just those 1,066 people (76%) that reported a time loss. Hence, the extrapolated per capital time burden is 1.21 hours (defined as 1.59 hours multiplied by 76%).

18. For purposes of a very conservative estimate for the value of lost time in responding to spyware infection on a desktop or laptop computer, I used the US minimum wage as of March 1, 2006 at $5.15 per hour. Assuming this hourly pay rate, the average extrapolated time-related cost impact of spyware is $6.24 (defined as 1.21 hours multiplied by $5.15 minimum wage hourly rate).

19. Drawing upon the above calculated values derived from sample data, I made the following inferences about the total cost impact on Web users that downloaded XCP and Media Max 5.0. Please note that I am basing this analysis on the following factors:

(a) Sample results can be used to approximate the two plaintiff classes with respect to the end-user spyware experience.

(b) XCP and Media Max 5.0 unleash spyware, causing approximately the same potential for malfunction and security threats for the end-user.

(c) One year, on average, is the approximate time impact for an individual in one of the two plaintiff classes.

(d) The approximate plaintiff class totals for XCP and Media Max 5.0 are 3 million and 4.2 million people, respectively.

(e) Of all CD purchasers, I assume that approximately 20% actually loaded their CDs onto their desktop or laptop computers. Hence, the number of XCP users that experienced a spyware infection is estimated at 600,000 individuals (3 million CD purchasers multiplied by 20%). The number of Media Max 5.0 users that experienced spyware is estimated at 840,000 individuals (4.2 million CD purchasers multiplied by 20%).

20. The following table reports the extrapolated total cost impact (expressed in U.S. million dollars) for two plaintiff classes:

SONY BMG DRM software categories	Million Web users	Monetary cost ($Million)	Time cost ($Million)	Estimated Cost Impact ($Million)
XCP	0.60	0.64	3.74	4.39
Media Max 5.0	0.84	0.90	5.24	6.14
Total	1.44	1.54	8.99	10.53

21. Assuming that the average U.S. wage rate published by the Department of Labor Statistics on March 30, 2006 is used instead of the minimum wage, the total estimated time cost would be $32.76 million dollars, and the total estimated cost impact would be $34.30 million dollars. These figures are based on an average reported weekly wage of $751 dollars and an assumed 40 hour average work week.

I declare under penalty of perjury under that the foregoing is true and correct. Executed this 6th day of April, 2006, at Elk Rapids, Michigan.

LARRY PONEMON

T:\CasesSF\Sony NY\DEC00029648.doc