Spyware: Looking Out for Consumers

By John Lawford and Dan McConville
Public Interest Advocacy Centre
1204 – ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

June 2006

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Canadian Cataloguing and Publication Data

Lawford, John
McConville, Daniel

Spyware: Looking Out for Consumers

ISBN 1-895-060-73-7

Executive Summary

Spyware is essentially software that limits users' control over their computers, and often is installed surreptitiously. Historically much of this type of software tracked users' online behaviour and delivered pop-up advertising, leading to the label "spyware". Its association with pop-up advertising and its difficult uninstall methods soon led to its reputation as an Internet scourge. "Spyware" as a broad category now includes many behaviours beyond spying, from the more 'innocent' displaying of advertisements right through to the delivery of viruses allowing for the remote control of the user's computer.

Over the last few years, spyware infection rates rose dramatically until their peak in late 2004. While there was a reduction in spyware installation rates between late 2004 and late 2005, likely due to Windows security patches, consumer education and advancements in anti-spyware software, infection rates again are climbing to near-record levels in the first quarter of 2006.

This trend is a serious threat, since spyware lowers consumer confidence in e-commerce, costs consumers tremendous amounts of time and money, and threatens governments and corporations with the possibility of large-scale security vulnerabilities. Spyware is also responsible for an increasing amount of service calls and computer crashes each year.

Extreme spyware activities likely violate several Canadian laws, including consumer protection legislation, PIPEDA, *Criminal Code* provisions, the *Competition Act* and the common law tort of trespass to chattels. However, neither remedies currently available to individual users nor deterrents to spyware producers are sufficient to address the problem. While intentionally deceptive or misleading installations are likely caught by several statutes, it is often selectively omitted information, rather than outright deceptive statements, that characterize the spyware installation process. It is uncertain if these more common behaviours are actionable, despite the fact that a large majority of computer users report having no knowledge of the software in question, or how it was installed. Government actors in Canada are not actively pursuing any enforcement activities against spyware companies on their own initiative at the moment.[1] This is likely due to a lack of resources or a view that spyware regulation does not fit the specific department's mandate.

[1] Note that the Canadian Internet Policy and Public Interest Clinic, together with the U.S. Center for Democracy & Technology filed parallel complaints with the Canadian Competition Bureau and U.S. Federal Trade Commission over the activities of one spyware operator and affiliated companies in November 2005. See CIPPIC and CDT Press Release at; http://www.cippic.ca/en/news/documents/Media_Release_Spyware_Complaint_Nov_3_2005.pdf

In this environment a legislative response may be necessary, but there is a major difficulty in regulating spyware: its lack of a cohesive definition. Any definition based on post-installation behaviours will ultimately leave significant discretion and potentially create unintended liability, because spyware behaviours can almost always have legitimate purposes in other contexts. Because of this limitation, the most appropriate legislative response should target the installation procedure, and require specific disclosures for potentially unwanted software behaviours that inhibit user control. This strategy will lead to a spyware definition built around the consent of the user, avoiding the need to outlaw specific software functionality and clarifying the emerging software installation regime.

Further regulation can rein in absurdly large affiliate networks, prevent the targeting of children to obtain installations, and perhaps pressure advertising companies to exercise more due diligence in controlling where their advertisements are displayed. Uninstall requirements could also be established, to eliminate misleading or ineffective uninstall procedures.

Critics of spyware regulation state that regulating bad actors on the Internet is impossible due to jurisdictional issues, or that additional notice will not affect user behaviour. Furthermore, legitimate software vendors likely fear overly broad legislation that could lead to unintended liability. While jurisdictional problems will always stand in the way of effective Internet regulation, this concern should not prevent spyware regulation since many large, established companies engage in spyware practices. These corporations can certainly be regulated with some success. The concern over additional notice similarly should not prevent regulation. While the relationship between notice and user behaviour may be questionable, uncertainty should not prevent legislators from establishing baseline standards to protect the public. Finally, legislation could be drafted in such a way as to minimize compliance efforts by legitimate software vendors, since most legitimate software will not engage in 'potentially unwanted' software activity. Generally any software that allows the user to control it will not be affected by legislation, and the vast majority of legitimate software allows the user to do so.

While US government actors have been criticized for their slow progress in tackling the threat posed by spyware, the Canadian government has done little concrete to date. Spyware nonetheless has been harming Canadian for several years and this inaction is becoming noticeable. Parliament should immediately determine which department is responsible for enforcing laws against spyware activity, and allocate the necessary resources to investigate and prosecute offenders. Spyware legislation, focused on the installation procedure, can then be introduced to aid in the fight, ensuring a strong reaction to the problem while minimally burdening legitimate software vendors.

While spyware has highlighted the need for clearer rules in software installation procedures, regulation of spyware should be viewed with a greater goal in mind: a stronger statement of users' rights over their computers. Users should always be presumed to desire complete control over their computer, and any attempt to limit that control through the installation of software should be done in a transparent fashion that requires fair and obvious consent.

This report therefore makes recommendations for a multi-facted approach to controlling spyware that includes regulation of certain aspects of spyware. In particular, this report recommends the following:

- Give a clear mandate and allocate resources towards the department best able to handle spyware complaints and enforce current laws against spyware activity.
- Enforce current consumer protection and competition laws against companies who engage in the worst spyware activity.
- Continue and strengthen consumer education initiatives regarding spyware, accentuating:
    - Only download from websites you trust;
    - Update your operating system software;
    - Install a trusted anti-spyware solution.
- Build support in the software community for clearer rules of installation for potentially unwanted software.
- Develop initiatives towards more accountability in the advertising industry, clarifying how advertising money gets to spyware distributors and what advertisers, advertising companies and brokers can do about it.
- Introduce spyware-specific legislation that:
    - Creates liability for software producers for the actions of their affiliates;
    - Clarifies the rules of installing potentially unwanted software by creating clear disclosure requirements;
    - Creates a higher threshold of consent for software installations than simple contractual consent, namely "fair and obvious" consent;
    - Creates a private right of action, with statutory damages, for unwanted installations of spyware;
    - Specifically empowers an agency with spyware enforcement and permits that agency to cooperate with foreign counterparts
    - Regulates the practice of targeting software installations towards children;
    - Requires standard uninstall procedures for all software;
    - Contains exemptions for operating systems.

Although spyware appears to be on its way to becoming a fact consumers are resigned to, the truth is that the dangers of its unchecked growth are too large to

ignore and the options for slowing its growth are both possible and not overly onerous. This report is a call to action on the part of consumers, governments and industry to work together to ensure consumers' computers remain useful and unpolluted.

Table of Contents

WHAT IS SPYWARE? 9

WHAT IS THE DIFFERENCE BETWEEN ADWARE AND SPYWARE AND DOES IT MATTER? . 9
THE DEFINITION OF SPYWARE USED FOR THIS REPORT 10
ARE COOKIES SPYWARE? 11
THE "ADWARE" BUSINESS MODEL, AND HOW IT BREEDS SPYWARE 12

WHY IS SPYWARE AN IMPORTANT ISSUE? 17

THE COSTS OF SPYWARE 17
Costs to consumers 17
Costs to business 18
THE EXTENT OF SPYWARE 19

SPYWARE JURISPRUDENCE AND PROPOSED LEGISLATION 22

PRIVATE ACTIONS 22
PUBLIC ACTIONS 23
CLASS ACTIONS 25
PROPOSED US LEGISLATION 26
LOBBYING ACTIVITY 28

IS SPYWARE LEGAL IN CANADA? 30

WHAT COUNTS AS CONSENT ONLINE? 31
Introduction 31
Online contract jurisprudence 31
Conventional contract law 33
Conclusion 35
CONSUMER PROTECTION LEGISLATION – ONTARIO 35
Definitions in the CPA 36
Unfair practices 36
New Internet agreement regulations 37
Conclusion 38
PIPEDA 38
TRESPASS TO CHATTELS 40
THE *CRIMINAL CODE* 41
THE *COMPETITION ACT* 42
CHILDREN AND SPYWARE 44
SUMMARY 44

JURISDICTIONAL ISSUES 45

INTERNATIONAL JURISDICTIONS 45
CANADIAN CONSTITUTIONAL LAW: FEDERAL OR PROVINCIAL JURISDICTION? 46
The trade and commerce power 46
The peace, order and good government power 47
The PIPEDA-model Approach 48

SUGGESTED REACTIONS **49**
ENFORCING CURRENT LAW 49
FUTURE REGULATION 50
REGULATING THE INSTALLATION PROCESS 51
What is potentially unwanted software? *52*
Will additional notice work? *53*
What kind of notice should be given? *55*
Consumer education *55*
Will the software industry support software installation regulation? *56*
Higher consent threshold *57*
OTHER REGULATORY CONCERNS 58
The "our affiliates did it" excuse *58*
Targeting children *59*
International cooperation *60*
Responsible advertisers *60*
INDUSTRY SELF-REGULATION 60
MARKET SOLUTIONS 62
A quick cookie fix *63*
CONCLUSION **64**
RECOMMENDATIONS **65**
APPENDIX I **66**
THE PURE SOFTWARE ACT: A PROPOSAL FOR MANDATORY SOFTWARE LABELING 66
APPENDIX II **68**
GOOGLE'S INTERNET EXPLORER TOOLBAR INSTALLATION 68
APPENDIX III **69**
PIAC SURVEY RESULTS 69

WHAT IS SPYWARE?

Unlike spam, the definition of spyware is very troublesome. It is well established that spyware is software that is downloaded onto users' computers, but this is where consensus on its attributes often ends. Industry groups have continually tried, and failed, to agree on a definition. There are several commonly accepted indices of spyware. These include:

- Installation takes place without the knowledge or consent of the user or with limited disclosure that prevents meaningful knowledge and consent.
- The software sends information about the consumer to external servers without the knowledge or consent of the consumer.
- The software takes away user control over browser or system configuration.
- The software does not allow the user to control when the software runs, or when and how the software updates.
- The uninstall procedure is either complicated, non-standard or may not exist at all. Sometimes the uninstall procedure may re-install the software, install other spyware, or cause system instability.
- The software is bundled with other files or software, and the user may not be given notice of all the software they are downloading.

These are merely indications of whether a piece of software may be spyware or not. There is no decisive software behaviour. As the Anti-Spyware Coalition (ASC) have demonstrated in their definition documents, once it is installed, almost every behaviour that spyware software exhibits can have a legitimate use as well.[2] In general the most consistent aspect of spyware is the lack of meaningful consent during the software's installation procedure.

What is the difference between adware and spyware and does it matter?

A major roadblock to consensus on a spyware definition is the "adware" industry. These companies developed an industry using installation techniques in the past that would easily attract the label "spyware", but in recent years some of them, especially WhenU, have cleaned up their practices to a great extent. Others, such as 180solutions, continue to use a business model that breeds non-consensual installations while pleading ignorance of its effects.[3]

Because these companies have been labeled spyware by many, they constantly distinguish between spyware and adware. The purpose of these

---

[2] The Anti-Spyware Coallition, *Definitions and Supporting Documents*, online: <http://www.antispywarecoalition.org/documents/definitions.htm>. [*ASC Definition Documents*].

[33] 180solutions openly advertises their use of an affiliate program on the partnering page of their website. Online at: <http://www.180solutions.com/pages/partners.aspx>. Last viewed on Dec. 15, 2005, the page read "ZangoCash, 180solutions [sic] affiliate program, has currently over 7,000 publishers distributing Zango software and earning incremental revenue."

categories is to distinguish "legitimate" software from "illegitimate" software. Adware is said to be a legitimate business, while spyware or malware constitute its evil relatives. It has been stated that adware only causes advertisements to be shown, while spyware tracks user behaviour,[4] but in fact many adware companies do track users' web surfing behaviour. Adware companies that track behaviour also frequently state that they do not transfer users' "personally identifiable information" (PII) to their servers. However, PII does not include a user's full browser history, all web searches performed by the user, the user's zip code, what software is on the user's computer, the user's software usage characteristics, or the user's system settings and preferences. Adware companies can record all of this information, while claiming not to transfer "personally identifiable information." Due to questionable definitions like these, the distinction between adware and spyware is generally not helpful in the spyware debate and only serves to confuse. The sole issue should be whether the adware is being installed with sufficient notice and user consent. If it is not, and the adware industry insists on referring to it as "adware", then it is both adware and spyware. Because non-consensual installations occur frequently in the adware business, the terms "spyware company" and "adware company" are used fairly interchangeably throughout this paper.

This is not to say that advertising supported software cannot exist. It can and does exist in various forms. The Eudora email program and Opera web browser are both offered free to users if users are willing to allow unobtrusive banner advertising within the program. However both of these applications only display advertising when the program is running, and they do not install additional software that tracks a user's web use or that runs without the user's permission. They also offer strong notice of their advertising functionality, and perhaps most importantly, they do *not* distribute their software through affiliates while offering pay-per-install incentives. These programs are examples of what legitimate advertising-supported software could look like.

The definition of spyware used for this report

While spyware obviously received its name from software that spied on users, for the purposes of this report spyware does not have to collect information about the user. Instead the broad, commonly used definition of spyware is applied. In this report, spyware is potentially unwanted software (software exhibiting behaviours that limit the user's control over their computer)[5] that is installed without adequate notice of the potentially unwanted functionality. The term spyware is therefore used to refer simultaneously to adware and spyware, provided the software has been installed without clear, prominent

[4] Webopedia, *The Difference between Adware and Spyware*, online: <http://www.webopedia.com/DidYouKnow/Internet/2004/spyware.asp>.

[5] Certain software behaviours take away user control over the software in question and their computer more generally. A preliminary list is available in the *Suggested Reactions* section under "What is potentially unwanted software?"

notice of its control-inhibiting behaviours. A spyware company, for the purposes of this report, is any company who's software exhibits potentially unwanted functionality and has been installed in this manner, either by the company itself or by an affiliate.

There is, however, a distinction drawn in this report between 'above ground' spyware companies, and 'underground' spyware companies. The former include large, well-funded corporations who established reputations as spyware vendors due to their lack of clear disclosures during installations over recent years and who today would be more likely referred to as adware companies. In contrast, the underground companies are usually smaller outfits who choose to hide from the spotlight rather than directly confront critics. While companies included in the 'above ground' spyware definition would vigorously refute their spyware label, their practices in the past have demonstrated installations through security holes or without adequate disclosure. Although their behaviours have in some cases improved, much of their fortune may rest on information collected without meaningful consent. This report concentrates on solutions to 'above-ground' spyware, however, the problems of 'underground' spyware are amongst the most egregious; it is understood that this report endorses the fullest enforcement of the present and any future criminal and consumer protection law against such operators.

Are cookies spyware?

Spyware legislation currently making its way through the US Congress is careful to specifically remove cookies from the definition of spyware.[6] Cookies are small text files that are uploaded to a user's computer, usually without the user's knowledge, and can be used by sites to maintain information about a user. For example the user can have her user name automatically filled in on a login form, or can be automatically logged on when she returns to a site through information maintained in a cookie.

Because of their useful features, cookies have become an integral part of the Internet's infrastructure. However, unless the user's browser has inconveniently high security measures, cookies are placed on the user's machine without the user's knowledge.[7] The potential also exists for advertising companies to plant a unique identifier on a user's machine using a cookie, and then use that cookie to track the user's browsing activity. This can be done because many online advertisements are actually 'sub-websites'; they are viewed on many different websites but their code originates from one single site.

[6] David McGuire "Congress Moving to Tackle Spyware Problem" *The Washington Post*, (15 April 2005.)

[7] In order to block a third-party cookie from most large advertisers with internet explorer, the user would have to set the security preferences to 'block all cookies' according to Eric Howes, an anti-spyware researcher, (interview conducted on June 28, 2005.) This setting would cause some web page features to be disabled, such as any 'log on' functions, and many web pages would not be displayed at all.

The advertising company that operates this site can therefore retrieve the same cookie anywhere that their advertisements appear on the web. These cookies are called 'third party cookies' since they are not set by the website being viewed. For the larger advertising companies whose ads are widespread, recording information from these cookies can amount to tracking a significant amount of a user's browsing activity. Hence a cookie can act like spyware in certain circumstances. These cookies are also known as tracking cookies.

Based on this potential functionality, anti-spyware applications offer removal of well-known tracking cookies. Cookies do not, however, pose an equivalent threat to downloaded executable files. While they can create significant privacy concerns, they cannot alter a user's computer settings in any way, and the user can easily remove them at any time. Due to these differences and their importance in web development, cookies should probably not be included in a general definition of spyware. However their privacy-invasive potential should be noted and users could benefit from more control over the notice offered when cookies are set on their machines. Anti-spyware software should certainly be allowed to report the existence of such cookies to users, and delete them if requested.

The "adware" business model, and how it breeds spyware

Spyware has flourished in the last two years because there is money to be made from it. Unlike virus writers, who often produce software for notoriety, certain types of spyware are designed to show advertisements to computer users, giving software developers an incentive to produce it. The most common business model[8] begins with software vendors developing programs that display advertisements and often record browsing habits. Once this software is installed, two sources provide revenue for the "adware" vendors. First, the vendor earns commissions for each time a user clicks on a displayed advertisement. This advertisement may be a pop-up ad, a sponsored search result in the case of search toolbars, or some other form of advertising. Second, if the spyware vendor is also collecting browsing information, this information can be sold to third parties for behavioural analysis or used for other profitable purposes.[9]

In order for companies to receive this revenue, however, end users must download their software, and normally users would not want software whose sole purpose is to track their behaviour and show them ads. To offer an incentive for users to download such software, spyware vendors either bundle their software with that of other software vendors, or create their own software to be offered

[8] Other models exist but are not practiced by the large 'above ground' companies. For example, a group of small companies collaborated to first infect as many computers as possible and then offer software that would solve the problem, for a price. The FTC is currently prosecuting several companies involved in this case.

[9] An example is Feedback Research, a division of Claria, online: <http://www.feedbackresearch.com>.

free to users along with their advertising and tracking software. Much of the software actually developed by spyware vendors is unnecessary,[10] or is offered at better quality for free by other developers.[11] This 'lure' software can come in many forms, including a screensaver, an Internet Explorer toolbar, a computer game, or even a media file. Spyware vendors may also give users the impression that installing their software is necessary to view an affiliate's website, when in fact simply using a browser other than Internet Explorer allows users full free access to the website content.

In this business model the primary revenue stream for a spyware company is heavily dependant upon the number of installations that the company's software obtains. Some spyware companies thrived by bundling with successful software producers to achieve significant numbers of downloads,[12] but alternatives were still sought to boost installation rates. Affiliate relationships were therefore established where independent website operators were offered a 'pay per install' commission that was sometimes hundreds of times the normal 'pay per click' rates for banner ads on websites. These rates have reached $5 per install in the past, but today usually lie between 20 and 40 cents.[13] For websites that can generate traffic, this pay-per-install revenue offers tremendous incentives to achieve installations with minimal or no user interaction whatsoever.

Companies have control to force the posting of a license agreement or other disclosures during their affiliates' downloads.[14] Adware companies can also easily bring their distribution in-house, as legitimate software vendors do. WhenU, a well known adware company whose reputation has improved significantly over the last year, brought almost all of their distribution in-house and virtually eliminated non-consensual installations of their software.[15] However since high install rates are crucial to the adware business model and

---

[10] For example, Claria continues to offer, as of the time of writing, a product called 'Precision Time Manager' which synchronizes a user's system clock, despite the fact that operating systems have such software built in. Online: <http://www.precision-time.com/>.

[11] Some spyware vendors offer a weather tracking application for the toolbar along with spying and advertising software, despite the fact that many weather websites offer far superior products for free or for unobtrusive advertising without causing popups. Other spyware vendors offer toolbars that are less effective and vastly more intrusive than free software, such as the Google toolbar which allows the user to turn off the potential 'spying' functionality when it is installed.

[12] According to Claria's prospectus for an IPO which did not occur, "a significant portion" of Claria's new users came from downloads of the Kazaa media desktop. Prospectus available online at: <http://www.hoovers.com/free/co/secdoc.xhtml?ipage=2723312&doc=0&attach=on>. [*Prospectus*].

[13] The top price-per-install at loudcash.com was $5 US when the site was viewed in July. Loudcash has since merged with ZangoCash, 180solutions' distribution website, and top price-per-install rates have dropped to $0.40. Online: <http://www.loudcash.com/>.

[14] Phone interview with Eric Howes, an anti-spyware researcher, on June 17, 2005. Mr. Howes is also a Microsoft MVP and a part-time consultant for Sunbelt software. [Hereafter *Howes*].

[15] WhenU's policies webpage states that one company policy is "No affiliate distribution, because it's impossible to police." Online at: http://www.whenu.com/overview_of_practices.html. A non-consensual WhenU installation has been documented since they initiated this practice, but overall there is little doubt of its success.

adware companies can easily 'pass the buck' of culpability on to their affiliates, these companies have had little incentive to change their practices. While they frequently claim to be trying to rein in poor installation tactics by affiliates, installs with minimal consent continue to occur. One major adware vendor, 180solutions, continues to actively employ at least 7000 affiliates, a system that clearly invites poor installation practices, despite the company's public relations rhetoric.[16]

The affiliate distribution model is also chiefly responsible for so-called "mega-bundles", where a vast number of adware applications are installed onto a user's machine. This practice earns the most money for affiliates, since they are paid for each successfully installed application, and can make an older computer completely unusable.[17]

The business model outlined above was followed by many of the well-known 'above ground' spyware companies, and has been successful. Claria, originally Gator, received a vast number of installs by bundling with Kazaa, the popular file-sharing program.[18] The company's current annual operating profit is approximately $35 million, and the company is valued at a minimum of $500 million.[19] 180solutions, as of April 2004, had already posted eight consecutive profitable quarters and almost $20 million in sales per year. They received $40 million of financing in April 2004.[20] DirectRevenue raised $20 million from venture capitalists that same month,[21] and WhenU received an additional $15 million in investment in July of 2005, raising their total financing to $35 million.[22] The private equity markets seem to be betting on adware's success.

Despite its financial achievements, the common adware business model has been heavily reliant on lack of regulation and oversight in the software installation process. Such an environment has allowed companies to achieve many installations with minimal disclosure, often using Internet Explorer security

---

[16] *Supra*, note 2.

[17] Chris Boyd "How not to install software" *Vitalsecurity.org* (5 July 2005), online: <http://www.vitalsecurity.org/2005/07/how-not-to-install-software.html>.

[18] *Prospectus*, *supra*, note 11. Apparently Claria achieved up to one quarter of their users (known to be around 40 million in mid-2005) through bundling with Kazaa: Stefanie Olsen "Adware's Second Act" *News.com* (July 12, 2005), online: <http://news.com.com/Adwares+second+act/2100-1024_3-5783948.html?tag=nl.caro> [*Olsen*]

[19] Pamela Parker "Claria's Next Move" *ClickZ News* (3 September 2004), online: <http://www.clickz.com/news/article.php/3403391>.

[20] John Cook "Internet advertiser disputes 'adware' label" *Seattle Post-Intelligencer* (2 April 2004), online: <http://seattlepi.nwsource.com/business/167416_180folo02.html>.

[21] Brad Stone "Invasion of the PC Snatchers" *Newsweek* (13 December 2004.)

[22] WhenU press release, (6 July 2005), online: <http://www.whenu.com/press_release_05_07_06.html>. While WhenU's behaviour has improved significantly under the leadership of Bill Day, nonconsensual installations have still occurred recently, and its business was established using the affiliate model, hence its inclusion in this list. *See* Suzi Turner "…And lose the balloons" *spywarewarrior.com* (24 November 2005), online: <http://netrn.net/spywareblog/archives/2005/11/24/and-lose-the-balloons/>.

exploits. Complicated uninstall procedures and the lack of advanced, accessible anti-spyware tools (which have appeared fairly recently) ensured that once an installation had occurred the software would be difficult, if not impossible, to remove. However, recent public outcry over deceitful tactics in the industry led many adware companies, including Claria, 180solutions, and especially WhenU, to offer more obvious disclosures and more straightforward uninstall procedures. It has been speculated that these reforms have significantly cut into the installation rates, and hence the revenues, of the 'above ground' companies.[23] Perhaps the contextual advertising side of the spyware business model is impractical when users actually know what the software does. The survey conducted by PIAC alongside this report asked participants if they would be willing to accept products commonly offered by adware producers along with their advertising and tracking software. In each case over 90% of users said they would not accept such a trade.[24]

Regardless of the possible failure of one source of revenue, the other source remains: the databases of browsing behaviour. In some cases companies have built enormous databases of users' browsing habits over the years. Claria maintains a database that is at least 12 terabytes, and potentially 20 or more.[25] Claria profits by selling behavioural analysis and data to third parties, and is reported to be testing a new behaviour-based Internet search application, which is being designed using information from their database.[26] Even if these companies fail to sustain their adware businesses, they could potentially be sitting on very valuable information, much of which was received through non-consensual installations in the past.[27]

One of the most important features of this business model is that the user is no longer the consumer in the traditional sense. Users provide no revenue to the adware companies. Instead, the user is the product: adware vendors are essentially selling the user's desktop, and thus the user's attention, to advertisers. In this model there are very few incentives to keep the user happy as a customer because the user is not really a customer at all. As long as advertisers or their brokers do not concern themselves with how ads are making their way to a user's desktop, there are plenty of incentives to get this type of software onto desktops through deceptive techniques.[28]

---

[23] One source suggests that WhenU's installations dropped by 50%: *Olsen*, *supra* note 17.
[24] *PIAC Spyware Survey* (Appendix III), questions 12(A) – 12(D).
[25] Matthew Hicks "Survey: Biggest Databases Approach 30 Terabytes" *eWeek.com* (8 November 2003), online: <http://www.eweek.com/article2/0,1895,1377106,00.asp >.
[26] "More behaviour based networks emerge" *Direct Marketing News* (April 2005), online: <http://www.dmn.ca/Articles/Articles/2005/april/behaviourbased.htm>.
[27] However Claria's prospectus stated that advertising was by far their chief revenue source, so it is uncertain whether these databases are very valuable, see *Prospectus*, *supra*, note 11.
[28] Thanks to David Fewer at The Canadian Internet Policy and Public Interest Clinic (CIPPIC) for this novel way of looking at the business model.

The perverse incentive scheme and lack of meaningful oversight in this market, along with the role-reversal of the traditional consumer, all contributed to make non-consensual installations a constant feature of the adware industry over the past few years. A quick look at any standard software and its distribution network demonstrates that it is possible to achieve the user's consent during every installation. However corporate policies that achieve this consent may be too detrimental to the adware business model to be voluntarily adopted.

In addition, there may be instances where the deliberate avoidance of informing the consumer and obtaining consent to a software process is the goal of digital rights management software. See *infra*, regarding the Sony BMG installation of rootkit software on consumers' computers with a simple CD install. Unconfirmed reports have also questioned the latest Windows XP "Microsoft Genuine Advantage" tool as it appears to report on all booting of Windows XP systems to assist with verification that illicit software has not been installed on otherwise valid XP installations. [29]

[29] See Lauren Weinstein's Blog, June 5, 2006 "Windows XP Update May Be Classified As "Spyware" and June 6, 2006 "Microsoft Responds Regarding Windows XP Update vs. Spyware". Online: http://lauren.vortex.com/

WHY IS SPYWARE AN IMPORTANT ISSUE?

The costs of spyware

Costs to consumers

It seems that everyone today has either been a victim of spyware or knows someone who has been. While the definition of spyware may be troublesome, like pornography, people know it when they see it. The symptoms are often a slow or frequently crashing computer, hijacked search and home pages, unwanted toolbars and most importantly, little or no user knowledge that the software would perform these functions. While surveys demonstrated that the spyware infection rate dropped since 2004, spyware infection rates recently have rebounded strongly, climbing 15% in the first quarter of 2006.[30] These statistics do not note the cause of the jump, however, one anti-spyware program vendor attributes it to consumers using 'free' anti-spyware tools (some of which are completely ineffective and even may install spyware) which do not the growing sophistication of spyware program.[31] Be that as it may, consumers are continuing to be vexed by spyware.

The cost of spyware is difficult to estimate and no concrete studies have been performed. The more benign forms of spyware can today often be uninstalled successfully using the add/remove programs window in the control panel, but often installations place numerous programs on the machine and users may have trouble finding every application. Others frequently require an anti-spyware application to remove them. This process sometimes costs the user money, and is almost always a significant time investment. Often anti-spyware scans must be repeated, with reboots in between each scan. In worst-case scenarios, hard drives must be re-formatted, which can cause the loss of valuable information. Many spyware victims have resorted to simply buying a new computer.[32] Dell has reported that spyware-related computer servicing rose from 2% of all calls to 15% from late 2003 to late 2004,[33] and Microsoft has reported that up to half of all Windows operating system crashes may be due to spyware.[34] Additionally, advertisements and browser hijacking that occur from spyware sometimes display adult content. Children may therefore be subject to viewing objectionable content without any user interaction whatsoever.

---

[30] Webroot Software Inc.,"State of Spyware, Q1 2006", p. 13.. Rate of spyware infection on consumer computers climbed to 87% in Q1 2006, after a drop to 72% in Q4 2005.
[31] *Ibid*., at p. 11.
[32] "Spyware pushes computer users to toss machines" *Marin Independent Journal* (17 July 2005.)
[33] Associated Press. "Spyware: Users Say Yes to It" *Wired*, (31 October 2004.)
[34] Siklos, Richard. "Can Gates and Spitzer protect you from spyware?" *The Daily Telegraph*, (1 May 2005.)

A study conducted by the Ponemon Institute indicated that 86% of respondents that reported having spyware installed stated that they suffered a monetary loss, productivity loss or inconvenience from the software. Of these respondents, 87% reported experiencing productivity losses and 34% reported being unable to use previously downloaded software.[35]

PIAC's own survey revealed similar trends. 54% of those with spyware infections stated that they had spent between one and five hours fixing their computer in the last six months, 19% spent between five and ten hours, and 10% spent more than ten hours.[36] 60% said they spent between zero and $50 to fix the problem, and 23% said they spent above $50 on repairs.[37] 51% of respondents stated that they required help from a friend or technician to rid their computer of spyware.[38]

37% of users who used an anti-spyware application to remove spyware reported that they paid for the software, and an additional 17% reported that they could not recall how much they spent on the software, so this number could be higher.[39] Of those who attempted to clean their computer with anti-spyware software, only 54% reported that the solution was effective in removing the spyware.[40]

While both PIAC's and Ponemon's survey results are based largely on the abilities of standard computer users to recognize and remember their spyware experiences, there is little doubt that they reveal a significant cost to consumers associated with unwanted software on home computers. In terms of time loss, productivity loss and actual dollars, spyware levies tremendous costs on Canadian computer users.

Costs to business

Businesses are perhaps hit even harder by the spyware threat. On top of current costs for enterprise virus protection and spam filters, most businesses require a spyware solution as well, which will likely be charged on a per-seat basis depending on the number of computers used in the business. Sharp increases in IT costs have accompanied the growth in spyware over the last several years. A survey of IT managers placed the average spyware cost at $130,000 per month.[41]

---

[35] The Ponemon Institute "National Spyware Study" (17 May 2005,) at 4, 13. [*Ponemon Study*].
[36] *PIAC Spyware Survey* (Appendix III), question 7.
[37] *Ibid*, question 8.
[38] *Ibid,* question 10.
[39] *Ibid*, question 11(B).
[40] *Ibid*, question 11(A).
[41] TechWeb News "Spyware Costs Weigh Heavy on IT" *InformationWeek* (2 August 2005), online: <http://www.informationweek.com/story/showArticle.jhtml?articleID=167100283>, and Linda Tucci "Spyware costs plague SMBs" *SearchSecurity.com* (18 May 2005), online: <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1092618,00.html>.

In addition to these costs are added the costs of lost productivity if a computer becomes unusable from spyware infections. These costs can be dramatic for employees with high hourly billing rates. Proprietary data or important work could also be damaged or lost in such an event.

The possibility of large scale corporate espionage has also been demonstrated recently following the discovery of a spy ring among Israeli companies using advanced spyware to steal sensitive corporate information.[42] American government departments are signing exclusive deals with Internet security firms in response to these dangers.[43]

Businesses can also suffer indirectly because of lower consumer confidence in e-commerce. A recent study by the Pew Internet and American Life Project demonstrates that Internet users are being more cautious online and may be limiting their use of online transactions partly due to the threat posed by spyware.[44]

The extent of spyware

The statistics on the spyware epidemic demonstrate that the tactics of spyware distributors are highly effective. An AOL and National Cyber Security Alliance online safety study conducted in October of 2004 indicated that 80% of the computers scanned contained spyware.[45] In addition the survey found 93 spyware components on the average infected computer, and the most found during a single scan was 1,059. Meanwhile only 20% of users knew adware was on their computer. 90% of those who had spyware or adware on their machines reported that they did not know what each of these programs were or what they did, and 95% said they had not given permission to anyone to install this software.[46]

A survey conducted by Webroot during the first quarter of 2005 found that 55% of business computers had some form of spyware installed. This number dropped from 74% in the last quarter of 2004, likely from increased use of

---

[42] TechWeb News "Nine Indicted In Israeli Spyware Espionage Case" *TechWeb.com* (8 July 2005), online: <http://www.techweb.com/wire/security/165700990>.
[43] Will Sturgeon "Spyware blocking deal signed by US Homeland Security" *Silicon.com* (24 May 2005.)
[44] Susannah Fox, Pew Internet and American Life Project, *Spyware: The threat of unwanted software programs is changing the way people use the internet* (Washington: Pew Internet and American Life Project, 2005.) [*Pew*].
[45] America Online and the National Cyber-Security Alliance "AOL/NCSA Online Safety Study" (October 2004) at 4. The practice of reporting the number of spyware 'components' on a computer is contentious, however, since the reported number may be interpreted as the number of pieces of spyware software when in fact one piece of software may comprise many components.
[46] *Ibid*, at 5.

spyware removal software[47] and the increased use of XP Service Pack 2, which closed many security holes in Internet Explorer.[48] In consumer machines 66% of computers were infected. These numbers again represent declines from 2004. The average infected consumer computer had 7.2 instances of spyware.[49] Webroot's webcrawler tool, which identifies spyware "in the wild" reported 79,754 traces of unwanted programs on the internet, an increase of eight-fold from the first quarter of 2004.[50]

Webroot released other surveys in the second and third quarters of 2005 which seem to indicate a downward trend in spyware installations. The percent of consumer PC scans with spyware (including tracking cookies) lowered from 88% in Q1, to 83% in Q2 and 72% in Q3[51] (Webroot did not report rates without tracking cookies in Q3, but approximately one quarter of each of these numbers is likely composed of cookies. Hence Webroot's spyware infection rates in Q3 are likely around 50% without tracking cookies.) Rates in enterprise PCs remained high, with 48% of computers containing adware,[52] now tracked separately from spyware, and 8% of computers containing sophisticated spyware that avoids detection from common anti-spyware programs.[53] Traces of spyware "in the wild" rose to almost 120,000 by Q3.[54]

However, Webroot's "State of Spyware – Q1 2006" report, referenced above, notes a strong rebound in all of these categories in 2006, to near record levels of infection. 87% of consumer PCs were infected in the first quarter of 2006 as opposed to 72% in Q4 of 2005, a 15% jump. Adware rates also jumped 24% between Q4 of 2005 and Q1 of 2006.

The Ponemon survey, conducted in 2005 as well, reported that 84% of respondents said their computers had been infected with spyware. Of these respondents 97% replied that they had not given permission for the download to occur, and 42% reported that they had no idea how the spyware was installed. 38% reported that they received the spyware by downloading free software. 35% also reported that they could not uninstall the spyware, and 60% of those who succeeded in un-installing reported that the process was either moderately difficult, difficult, or very difficult.[55]

---

[47] Webroot. *The State of Spyware Report, First Quarter, 2005*, (Boulder, Co: Webroot, 2005) at 22 –34. [*Webroot Q1*]
[48] "WhenU Awareness, One Year Later" *PC Pitstop*, (May 2005), online: <http://www.pcpitstop.com/spycheck/whenu2.asp>.
[49] Webroot Q1, *supra* note 43.
[50] *Ibid,* at 40.
[51] Webroot, *The State of Spyware Report, Third Quarter, 2005*, (Boulder, Co: Webroot, 2005), [*Webroot Q3*].
[52] *Ibid*, at 39.
[53] *Ibid*, at 37.
[54] *Ibid*, at 26.
[55] *Ponemon Study* at 11-12.

PIAC's survey demonstrated similar high numbers. 57% of participants reported that they had had spyware on their home computer,[56] and almost half of those stated that they had more than 3 infections in the past six months.[57]

Inconsistencies in survey data can be attributed to both differences in definition and relying on participants to judge for themselves if they have had spyware installed on their PCs. Overall, there was a short-lived declining trend in the infection rate in 2004-5, but spyware again is on the rise and it continues to contaminate a huge percentage of computers. Security patches to Windows XP, improving anti-spyware applications and consumer education have all likely played a role in stemming the tide during 2004-5, but it appears unlikely that these solutions will continue to offer long-term relief without more concerted action by governments, consumers and business.

[56] *PIAC Spyware Survey* (Appendix III), question 5.
[57] Ibid, question 6.

SPYWARE JURISPRUDENCE AND PROPOSED LEGISLATION

Private actions

Spyware companies have attracted litigation in the past, but much of this litigation was initiated by businesses with web sites that were being flooded with pop-up ads from downloaded spyware. Consumers and government actors were much slower to take action. Unfortunately most of the inter-business litigation was based mainly on trademark infringement and has since been settled, so no significant jurisprudence has emerged to judge the actions of spyware companies or their installation procedures.

In 2001 Gator was sued by a variety of companies alleging trademark infringement, including UPS, Tigerdirect, Lending Tree, Extended Stay and Six Continents Hotels. In 2002 they were sued by another group, including the Washington Post and New York Times, who won a preliminary injunction against Gator but settled out of court soon afterward.[58] All the above suits had been settled by 2004 according to a clerk of the court hearing in 2004.[59]

Similar private actions were initiated against WhenU, with mixed success. One case brought by U-Haul was dismissed in a summary judgment, [60] another brought by 1-800-Contacts against both WhenU and a company that advertised with WhenU led to a preliminary injunction against WhenU but eventually failed.[61] At least one similar suit has been brought against 180solutions.[62]

In terms of computer users suing software vendors for spyware behaviour, only two individual actions have occurred. A North Dakota lawyer, John Gosbee, commenced a private action against three fraudulent anti-spyware companies and the companies' owner. The case was thrown out at trial in January for lack of evidence, but is currently being appealed. A similar case, in which the same alleged spyware vendor was sued by attorney Glenn McCandliss in Michigan, resulted in a settlement of $2000.[63] The defendants infected PCs with spyware and then offered anti-spyware software for sale to clean the infected computer.

---

[58] Stefanie Olsen "Web publishers settle with Gator" News.com (7 February 2003) online: <http://news.com.com/2100-1023-983870.html >.
[59] Ben Edelman "Pending Suits against Designers of Spyware" *benedelman.org*, online: <http://www.benedelman.org/spyware/#suits>.
[60] *U-Haul International Inc. v. WhenU.com Inc*. 2003 WL 22071556, online: <http://cyber.law.harvard.edu/people/edelman/ads/whenu-uhaul-summaryjudgment.pdf>.
[61] *1-800 Contacts Inc. v. WhenU.com Inc*. Docket Nos. 04-0026-cv and 04-0446-cv (2d Cir. June 27, 2005), online: <http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-10121.PDF>.
[62] *Supra* note 55.
[63] Documentation of this case is on file at PIAC.

Public actions

Several high profile public actions have recently been filed against spyware companies in the United States. New York attorney general Elliot Spitzer filed a suit against Intermix Media of California, while the Federal Trade Commission filed complaints against several companies for spyware activity. Most of the FTC's complaints were based on 'unfair' or 'deceptive' business practices under the FTC Act.[64] Spitzer's claim came under both the New York State General Business Law, which prohibits false advertising and deceptive business practices, and the common law tort of trespass to chattels.[65] No spyware-specific legislation was applied, or available, for these claims. Spitzer established a permanent Internet bureau in his office in December of 2000, and it was research from this bureau that led to the conclusion that 3.7 million downloads of Intermix software from more than ten websites were directed at New Yorkers alone.[66] The suit was settled in the summer of 2005 with Intermix paying $7.5 million but admitting no wrongdoing.[67]

In late 2004 the FTC sued Seismic Entertainment Productions and their affiliates for distributing spyware.[68] The action was filed under the Federal Trade Commission Act, which prohibits the use of "unfair methods of competition" and "unfair or deceptive acts or practices … in affecting commerce."[69] The FTC succeeded in obtaining a preliminary injunction against Seismic, based on a finding that it was likely the FTC would win the case.[70] In May, 2006, the FTC succeeded in its suit against Seimic Entertainment Productions, obtaining a default court order against Sanford Wallace and his company Smartbot.Net that ordered the defendants to pay over $4 million to the FTC and effectively barred them from the spyware business. A settlement with a related ad-broker resulted in another $250,000 payment.[71]

The FTC also pursued Odysseus Marketing, a company that offered peer-to-peer software allegedly bundled with spyware that installed many other programs causing pop-up ads and corrupted search results when popular search

---

[64] *Federal Trade Commission Act*, U.S.C. tit. 15 § 45 (1914).
[65] New York Attorney General, Verified Petition against Intermix Media (April 2005), online: <http://www.oag.state.ny.us/press/2005/apr/Verified_Petition.pdf>.
[66] Associated Press "New York Sues Internet Marketer over 'Spyware.'" *The New York Times* (28 April 2005.)
[67] Reuters "Intermix settles spyware lawsuit" *MSNBC* (14 June 2005), online: <http://msnbc.msn.com/id/8219505/>.
[68] *Federal Trade Commission v. Seismic Entertainment Productions, Inc., et al*. 2004 U.S. Dist. Lexis 227788 (D.N.H., October 21, 2004) online: <http://www.phillipsnizer.com/library/cases/lib_case358.cfm>.
[69] *Ibid*.
[70] *Ibid*.
[71] FTC Press Release, *Court Halts Spyware Operations* (4 May 2006), online: <http://www.ftc.gov/opa/2006/05/seismic.htm>. Full text of the Order online: <http://www.ftc.gov/os/caselist/0423142/WallaceFinalJudgment.pdf>.

engines are used. These activities are again alleged to violate the unfair and deceptive practices provisions.[72] In May 2006, the FTC obtained a revised preliminary injunction barring Odysseus Marketing and its principal, Walter Rines, from among other things, collecting personal and web browsing habit information from web surfers that they aggregated and sold. The revelation that personal information collection and sale was a major goal of the spyware operations was a serious new development, confirming as it did that 'spyware' really could be used to monitor computer users and provide personal information about them to third parties.

Finally, the FTC's brought charges against Enternet Media, which resulted in a temporary restraining order, preventing the company from disseminating any software code that interferes with consumer's computer use.[73] Enternet Media was notorious as the source of "Elitebar" and "SearchMiracle", programs that were often installed without user consent.

The FTC also recently settled a suit against Advertising.com for distributing SpyBlast, a security program that was installed with software that displayed pop-ups and tracked the user's browsing. The additional software was only disclosed in a EULA that the user was not forced to view during the installation procedure. The FTC staff memo argued that the installation of ad-supported software is a material fact in the installation, and the failure to adequately disclose this fact is a deceptive act or practice.[74]

The outcome of the FTC cases against Seismic and Enternet Media has created some positive jurisprudence for spyware actions. While Seismic's actions were extreme, Enternet's were fairly standard for spyware vendors. The strong stance taken by the FTC against Advertising.com, and the speed with which the suit was settled, also indicate that a failure to obviously disclose the bundling of advertising software is a deceptive practice according to the Federal Trade Commission Act (FTCA). The FTC could significantly improve installation procedures using existing law if its broad reading of the FTCA is accurate. It should be noted however that the Canadian Competition Act does not have the same strong consumer protection measures contained in the FTCA. The FTCA outlaws both deceptive and "unfair" practices, while the Competition Act only

---

[72] FTC Press Release, *FTC Seeks to Halt Illegal Spyware Operation* (5 October 2005), online: <http://www.ftc.gov/opa/2005/10/odysseus.htm>.

[73] See *Federal Trade Commission Plaintiff*, v. *Enternet Media, Inc. , a California corporation, Conspy & Co., Inc., a California corporation; Lida Rohbani, individually and as an officer of Entemet Media, Inc. and Conspy & Co., Inc.; Nima Hakimi, individually and as an officer of Entemet Media, Inc. and Conspy & Co., Inc.; Baback (Babak) Hakimi individually, doing business as Networld One, and as an officer of Entemet Media Inc. and Conspy & Co., Inc.; and Nicholas C. Albert, individually and doing business as Iwebtunes and www.iwebtunes.com*, Defendants. Civil Action No.: CV05-7777CAS (AJWx), File No. 052 3135. Online: http://www.ftc.gov/os/caselist/0523135/0523135.htm

[74] U.S., Federal Trade Commission. Complaint against Advertising.com (042-3196) (2005), online: <http://www.ftc.gov/os/caselist/0423196/050803comp0423196.pdf>.

refers to deceptive or misleading practices. Spyware installations could be labeled unfair with far greater certainty than they could be labeled "deceptive".

Class actions

A final legal strategy is the class action lawsuit, which has recently been pursued against several adware companies. The first, against DirectRevenue, was brought under the common law tort of trespass to chattels as well as the Illinois Consumer Fraud Act, based on the company's installation and uninstall procedures.[75] The Illinois Consumer Fraud Act prohibits "unfair or deceptive acts or practices."[76] The action also seeks remedies for unjust enrichment, negligence, and the Illinois Criminal Code offense of computer tampering, which allows a civil action by anyone who suffers damage from the crime.[77] The claim has not yet gone to court as of the time of writing.

Class actions have also been launched against 180solutions, a well known adware company whose non-consensual software installations have been documented numerous times. In September, 2005, the Collins Law Firm (the same firm that filed against Direct Revenue) launched the first of these suits, claiming trespass to chattels and negligence, as well as violations of the U.S. Electronic Communications privacy Act, the Consumer Fraud Act, and state specific legislation.[78]

Another class action also exists against eXact Advertising alone, which makes similar claims to those above,[79] and a final class action filed in California by Bronson & Associates names each of 180solutions, eXact Advertising and DirectRevenue as defendants.[80] Claims in this complaint include trespass to chattels, violations of consumer protection legislation and fraud.

In late 2005 at least five class actions were filed against Sony BMG and First 4 Internet for their use of digital rights management software that hid itself from the operating system and installed without consent when users attempted to play certain CDs on their computers. The DRM software was not disclosed in the EULA or during the installation process, nor were any of its suspicious

---

[75] *Stephen Sotelo v. DirectRevenue LLC*, No. 05 C 2562 (N.D. Ill., 8/29/05), complaint at para 27-38, online: <http://www.courtbriefs.com/PDF_Files/CCCOOK05CH05883CA.pdf>. Decision regarding motion to dismiss available at: <http://sunbelt-software.com/ihs/alex/drruling.pdf>. [*DirectRevenue*]

[76] *Ibid* at para 33.

[77] *Ibid* at para 46 – 57.

[78] Suzi Turner "Lawsuit filed against 180solutions" *Spyware Confidential* (13 September 2005), online: <http://blogs.zdnet.com/Spyware/?p=655>. Case citation: *Simios v. 180solutions Inc*., No. 05 C 5235 (N.D. Ill., 9/13/05).

[79] *Michaeli v. eXact Advertising*, No. 05 CV 8331 (S.D.N.Y. 09/27/05), complaint online: <http://www.spywarewarrior.com/eXact-complaint.pdf>.

[80] Suzi Turner "Lawsuit against 180solutions, DirectRevenue and eXact Advertising" *Spyware Confidential* (20 December 2005), online: <http://blogs.zdnet.com/Spyware/index.php?p=730>.

behaviours. Causes of action included trespass to chattels, fraud, violations of consumer protection laws and violations of state-specific spyware laws.[81]

The class action against DirectRevenue, the sole class action that has been to court at the time of writing, has given positive signs regarding the success of the trespass to chattels tort in a case against spyware. In rejecting Direct Revenue's motion to dismiss, Judge Gettleman stated that "[i]n recent years, trespass to personal property, which had been largely relegated to a historical note in legal textbooks has reemerged as a cause of action in Internet advertising and e-mail cases."[82] The judge went on to say that causing users' frustration and the slowing down of their computers could amount to the damage necessary in an American trespass to chattels claim.[83]

While there have been several claims filed against spyware companies recently, the prevalence of settlements and the slow development of the common law have limited the emergence of jurisprudence and clarification of the law of software installations. The numerous class actions making their way through the courts provide some hope that meaningful US jurisprudence regarding spyware will come forth, but this process will take much time, and there remains the possibility that these cases will fail.

Proposed US legislation

Four spyware bills have been put forward in the US Congress over the last few months. The I-SPY Act[84] and Spy Act[85] were introduced in the House, and the SPY BLOCK Act[86] was introduced in the Senate. An enhanced consumer protection bill focusing on spyware was also introduced.[87] Twenty state spyware bills are also currently being considered, although they will not be reviewed in this report.[88]

The I-SPY Act is a short act that creates offenses for accessing a computer without authorization in furtherance of another offense, and for obtaining or transmitting personal information or impairing the security of that computer without authorization. While the act creates new offenses, their

---

[81] Mark Lyon "Class Action Lawsuits" *SonySuits.com* (30 November 2005), online: <http://www.sonysuit.com/classactions/>.
[82] *DirectRevenue*, *supra* note 69, at 16-17.
[83] *Ibid*, at 17-18.
[84] U.S., Bill H.R. 744, *Internet Spyware (I-SPY) Prevention Act of 2005*, 109th Cong., 2005. [*I-SPY Act*].
[85] U.S., Bill H.R. 2929, *Securely Protect Yourself Against Cyber Trespass Act*, 109th Cong., 2004. [*Spy Act*].
[86] U.S., Bill S. 2145, *Software Principles Yielding Better Levels of Consumer Knowledge Act*, 109th Cong., 2004. [*Spy Block Act*].
[87] U.S., Bill S.1004, *Enhanced Consumer Protection Against Spyware Act of 2005,* 109th Cong., 2005.
[88] Webroot. The State of Spyware Report, Second Quarter, 2005 (Boulder, Co: Webroot, 2005) at 9.

effectiveness is questionable since it is begging the question: When has a piece of software achieved authorization? This bill does nothing to clarify that question, and may as a result do very little to improve the spyware problem.

The Spy Act, probably the most well known of these bills, was re-introduced this year after the Senate failed to ratify it in 2004. Its main provisions lie in sections 2 and 3. While section 2 demonstrates the same limitations as the I-SPY act, section 3 contains stronger notice and consent provisions. Section 2 of the bill prohibits unauthorized 'unfair and deceptive acts or practices' that turn a computer into a 'spambot', hijack a browser, dial out using the modem or internet connection, or deliver 'advertisements that a user… cannot close without undue effort.' Section 2 also prohibits unauthorized keystroke logging, phishing and pharming activities. These provisions suffer from the same problems as the I-SPY act. Each of these activities is likely already illegal. The bill even states that such activities only violate the act if they are conducted through 'unfair or deceptive acts or practices': language that is identical to that used throughout consumer protection legislation and in the FTCA. The first part of this bill focuses on post-installation spyware behaviour rather than on how the software became installed.

Section 3 of the Spy Act addresses notice and consent requirements during installation. It requires notices to be displayed (sample notices are included but 'substantially similar' versions are allowed) in order to install any software on a computer that collects certain types of information or offers contextual advertising. This section also requires that such software contain certain functions, such as an uninstall function and an 'identity' function that ensures that every ad offered clearly states which program caused it to be displayed. These provisions are helpful, but still only apply to certain types of potentially unwanted software. Some toolbar and adware programs do not transmit information back to their home servers, and hence do not have to meet the notice and consent requirements or the requirements for an uninstall or identity function. These types of software should be held to similarly high standards, since they often install without the consent of the user and perform other unwanted functions, such as running on startup, re-installing, or launching pop-ups.[89] While the Spy Act is a step up from the I-SPY Act, it suffers from significant drawbacks.

The SPY BLOCK bill as introduced in the Senate in the 108th Congress was a strong piece of legislation that correctly placed emphasis on the installation procedure as the cornerstone of the spyware definition, and contained thorough notice requirements for particular software functions. The bill was then essentially re-written in committee, with the notice requirements removed. The original bill required software to "include a separate disclosure, with respect to each information collection, advertising, distributed computing, and settings

[89] Ben Edelman "Ask Jeeves Toolbar Installs via Banner Ads at Kids Sites" *benedelman.org* (9 May 2005), online: <http://www.benedelman.org/spyware/installations/askjeeves-banner/>.

modification feature."[90] The bill set out guidelines for achieving user consent and prohibited any installation that occurred without providing required notices and receiving consent. The bill further prohibited poor or non-existent uninstall procedures.

These strong features of the original bill were almost all struck out in committee. The bill as it came out of committee, and as it was re-introduced in the 109th Congress, exhibits many of the flaws of its counterparts. It prohibits misleading or materially false notices, essentially duplicating consumer protection legislation, and it prohibits 'unauthorized' spam-bot creation, browser hijacking, invasive pop-ups and covert setting modification. To its credit the bill clarifies installation requirements for information collection features, similar to the Spy Act. The SPY BLOCK act is once again undergoing review in committee as of the time of writing.

The enhanced consumer protection bill offers similar provisions, barring "deceptive" installations, which are likely already contrary to the FTC Act, and clarifying jurisdictional provisions for the FTC.

The U.S. bills also do not clearly define an agency relationship between a software vendor and its distribution affiliates. Software vendors must be liable for their affiliates' actions, or in many cases they could dodge liability for non-consensual installations on the basis that the affiliate was chiefly to blame. Realistically it is the practice of using absurdly large affiliate networks that is responsible for these installations, as they are virtually certain to occur with the incentive scheme in place. It could be years until the courts conclusively deal with this issue in case law.

While these new acts demonstrate that Congress is taking the spyware problem seriously, they fail to adequately address what constitutes an unauthorized or deceptive installation. Instead they focus on particular post-installation activities like browser hijacking or setting modification – activities that could be desirable if the software was installed with appropriate consent. The sole bill that attempted to lay ground rules surrounding notice and consent had these strong provisions struck out in committee, and none effectively address the affiliate problem.

Lobbying activity

As a result of impending spyware legislation, adware companies, along with more mainstream technology companies, were actively lobbying the US government in 2004. WhenU listed all three spyware bills in their lobbying documents, and spent $260,000 in lobbying efforts. As of the first half of 2005 they had spend $160,000 on all four bills.[91] Claria listed the I-SPY and the Spy

[90] *Spy Block Act*, at s. 3(a)(2).
[91] US Senate Lobbying Report, Whenu.com, online at:

Block bill, and reported spending $520,000 in the second half of 2004. They listed all the bills in their 2005 documentation and spent $120,000 in the first half of the year.[92] 180solutions also lobbied all four spyware bills, and spent $225,000 in 2004 and $100,000 in the first half of 2005.[93] Google listed spyware as one of their lobbying concerns, spending less than $60,000 on the issue, and Dell spent $20,000 in lobbying the spyware bills amid recent controversy over their bundled software.[94] It is somewhat uncertain what interest Google and Dell have in spyware legislation. Google is likely concerned about the potentially unwanted features of some of its software that may record user behaviour. The tremendous lobbying action by adware companies (Claria, 180solutions and WhenU) is almost certainly an attempt to dilute the bills or to prevent them from becoming law.

It is impossible to say what impact these firms have had in their lobbying efforts. However, the high sums of money being spent, the severe amendments made to the SPY BLOCK bill and the fact that none of the spyware bills passed through the senate in 2004 point to the conclusion that the private interests have been successful. Regardless of its effect, there is undoubtedly a significant private interest attempting to influence the spyware law that may emerge from Congress.

<http://sopr.senate.gov/cgi-win/m_opr_viewer.exe?DoFn=3&CLI=WHENU.COM&CLIQUAL==/>. Note: Hard copy versions of these documents are on file at PIAC. Full year numbers are calculated by adding the amount listed in the mid-year report (January to June) to the amount listed in the year-end report (July to December).

[92] US Senate Lobbying Report, Claria Corp, online at: <http://sopr.senate.gov/cgi-win/m_opr_viewer.exe?DoFn=3&CLI=CLARIA%20CORP&CLIQUAL==/>.

[93] US Senate Lobbying Report, 180solutions, online at: <http://sopr.senate.gov/cgi-win/m_opr_viewer.exe?DoFn=3&CLI=180SOLUTIONS&CLIQUAL==/>/

(180 Solutions filed with two separate lobbyists. The amount above is the sum of all expenses reported.)

[94] John Leyden "Dell rejects spyware charge" *The Register* (15 July 2005), online: <http://www.theregister.co.uk/2005/07/15/dell_my_way_controversy/>.

IS SPYWARE LEGAL IN CANADA?

The method used to install spyware on a user's machine can violate many Canadian laws, including consumer protection acts, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the *Criminal Code*, the *Competition Act* and the common law tort of trespass to chattels. While criminal convictions and public actions under provincial consumer protection acts could be successful against spyware producers, neither action has been attempted to date. A private action could rely upon breach of a consumer statute but also likely would allege trespass to chattels. With this cause of action, its success would depend upon the court's view of whether the download was 'unauthorized.' In worst-case scenarios the download is clearly unauthorized, but in others it may not be, or may be difficult to prove, particularly when a license agreement has been displayed.

Software downloads, including spyware, are usually governed by a licensing contract between the user and the software vendor, called an End User License Agreement (EULA). This contract is generally shown to the user on the screen before the installation takes place, and the user must click a button to confirm their assent to the agreement.[95] Contracts of this sort are known as 'clickwrap'. The legal status of clickwrap contracts is somewhat uncertain due to the limited jurisprudence of online contracting and the difficulties associated with applying conventional contract law to this new medium. Their legal nature is important however, since it may decide whether the installation is authorized. When no EULA or similar disclosure is displayed during an installation, it may be that the installation violates current laws in Canada. Even if a EULA is used to disclose potentially unwanted software activity, when considered in light of the ruling in *Tilden Rent-a-Car v. Clendenning*,[96] the user may not have assented to every term by simply clicking 'I agree' in these situations.[97]

---

[95] *Specht v. Netscape Communications Corp*. 00 Civ. 6249 (S.D.N.Y. 2001), [*Specht*].
[96] *Tilden Rent a Car v. Clendenning* 18 O.R. (2d) 601. [*Tilden*].
[97] This difficulty has been appreciated by legislators in Canada already. For example, the Ontario *Consumer Protection Act, 2002*, s. 38 requires, with regard to Internet (clickwrap) contracts that consent must be clearly given: "The supplier shall provide the consumer with an express opportunity to accept or decline the agreement and to correct errors immediately before entering into it." This provision is of limited value to the consumer at the moment, as it does not apply to contract with a value of less than $50, which includes most spyware.

What counts as consent online?

Introduction

When considering 'drive by' downloads[98] and deceptive or misleading EULAs, there is little doubt that the software producer does not obtain the user's consent to install the software. Many underground spyware companies and affiliates of above ground spyware companies engage in these practices regularly to install software, and their actions are almost certainly illegal according to Canadian law outlined below. However most above ground spyware companies have largely discontinued the worst of these practices and rely instead on lengthy EULAs and social engineering[99] to obtain consent. The major issue surrounding the legal standing of these agreements is to what extent a software company can rely on the user's clicking of 'I agree' next to a lengthy and complex EULA. Does this action impute knowledge of the entire contents of the EULA to the user? Does it mean the user has consented to the behaviour of all software mentioned in the EULA?

The answer to both these questions, despite the apparent deceitful nature of the companies' actions, could be "yes." No legislation or jurisprudence specifically addresses the problem in the spyware context, and until such law comes forth, spyware producers can continue to rely on this legal limbo to claim consumers consent to their actions.

This issue will be decided in reference to contract law. In this branch of law, once a contract has been signed, there is a presumption that the contract is binding, and the parties are aware of its contents.[100] Any party wishing to negate any of the contractual terms is responsible for establishing why the contract, or the term in question, should not be upheld. As demonstrated below, clicking an 'I agree' button on a EULA is considered signing a contract, so knowledge of the entire contents of the EULA is assigned to the user with this action. In order to claim that a download was unauthorized after a EULA was displayed, the user must establish a legal reason why the contract should not be binding.

Online contract jurisprudence

Specht v. Netscape Communications Corp.,[101] a US case, clarified under US law that users must either 'manifest their assent' to a EULA by performing some action, such as clicking an 'I agree' button next to the EULA, or at the very

[98] A 'drive by' is when a download occurs with no notice given to the user at all. It is often achieved using Internet Explorer's ActiveX controls. The term is also sometimes used for ActiveX downloads in general.
[99] For example, relying on novice computer users to simply click 'ok' without understanding what they are agreeing to.
[100] *L'Estrange v Graucob*, [1934] 2 KB 394, (U.K.) [*Estrange*].
[101] *Specht, supra* note 89.

least users must be made aware that they are entering a contract, made aware that the terms must be agreed to and made aware of where the terms can be read.[102] A Canadian court likely would come to a similar conclusion. Based on this precedent, spyware producers who do not present a EULA or make the user aware of a contract would likely be unable to rely on any alleged contract. *Moore v. Microsoft*, another American case, reinforces this conclusion. In that decision the entire EULA was considered binding since the user clicked an 'I agree' button to confirm assent.[103]

In both the Ontario case of *Rudder v. Microsoft Corp*[104] *(Rudder)* and the New Jersey case of *Caspi v. The Microsoft Network LLC*[105]*(Caspi,)* clickwrap clauses were again upheld as legitimate contract clauses. The judge in *Rudder* found that contract terms that were not present in the visible area of a scroll box did not make such terms analogous to 'fine print.' The plaintiffs were attempting to rely on some terms of the agreement while attempting to discount others, weakening their argument that they had not received notice of the terms in question. However in both *Caspi* and *Rudder*, the analogy to fine print was discounted based on the logic that there is no distinction between the font in which the clauses were printed. The judge in *Caspi* stated "To conclude that plaintiffs are not bound by that clause would be the equivalent of holding that they were bound by no other clause either, since all provisions were identically presented." This holding would lead to the conclusion that users are bound by all disclosures hidden within lengthy EULAs.

Kanitz v. Rogers,[106] an Ontario case, gave more indication as to what 'awareness' of the contractual terms entailed, when the Court allowed an amendment to a contract through notice given on the defendant's website. The amendment clause in the original contract specifically stated that notice could be given on the website, and the Court ruled that based on this clause it was expected that the customers should check the website from time to time to notify themselves of any changes. Nordheimer J. quoted the *Rudder* decision to support the logic that no 'fine print' can exist in EULAs.[107]

The *Kanitz* decision undermines important principles of contract law. For example, a EULA could state that the program in question collects no personally identifiable information, and that any information the program collects must be treated in line with the company's privacy policy, with a link to the policy. *Kanitz* suggests that another term in the contract could then state that all terms of the

---

[102] The judge in *Specht* quoted a California decision that sums up his judgment well: "an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious." *Windsor Mills, Inc. v. Collins & Aikman Corp.,* 101 Cal. Rptr. at 351. (U.S.)
[103] *Moore v. Microsoft Corp*., 293 A.D.2d 587 (U.S).
[104] *Rudder v. Microsoft Corp.* [1999] O.J. No. 3778.
[105] *Caspi v. The Microsoft Network LLC,* 732 A.2d 528 (U.S.)
[106]*Kanitz v. Rogers,* [2002] O.J. No. 665. [*Kanitz*].
[107] *Ibid,* at para 30.

EULA are subject to change and new versions are available on the company's website. The company could then post an altered contract on the website indicating that their program now collects personally identifiable information, and that their privacy policy has been altered to allow the sale of information to third parties. This practice may achieve the user's assent according to *Kanitz*, yet it seems to fly in the face of an underlying principle of contract law – certainly no 'meeting of the minds' has occurred in this situation. Many spyware companies now include similar amendment clauses in their EULAs,[108] in the hopes that *Kanitz* will be applied in their jurisdictions.

Conventional contract law

While judicial logic has so far successfully determined that fine print cannot exist in EULAs, average computer users recognize that practically this cannot be the case. EULAs are not often read by end-users,[109] due to their legalistic language and length. In many instances it is obvious that software vendors take advantage of users' unwillingness to read these contracts by disclosing very important information, of which the user is unaware, in the middle of a lengthy, complex agreement. It seems almost certain that a reasonable person, when presented with the worst abuses of these buried EULA disclosures, would conclude that they are analogous to fine print. If judges refuse to accept this analogy, then the concept of 'burying terms' in an online agreement has no legal significance. This conclusion seems highly unreasonable and reminds one of the draconian contract law that emerged from *L'Estrange v. Graucob*.[110]

It is in this respect that traditional contract law can be applied to online contracts to clarify their legal authority. Perhaps the most relevant Canadian case in this respect is *Tilden Rent a Car v. Clendenning (Tilden,)*[111] where the Ontario Court of Appeal held that a signature could not be relied on as manifesting assent when it is not reasonable for the party relying on the document to believe that the signer really did assent to its contents. Mr. Justice Dubin stated that it was unreasonable in the circumstances since the type of contract in question was usually conducted in a rushed fashion and the terms in question were particularly onerous and difficult to discover (they were in fine print on the back of the document.) He concluded that in these circumstances such terms must be drawn to the consumer's attention to be enforceable. There are many parallels between the contract in *Tilden* and lengthy, complex EULAs. Those who offer EULAs are likely to recognize that they are often accepted by users in a rushed fashion and rarely, if ever, read. They are standard form 'take it or leave it' contracts that the user cannot negotiate. As detailed above,

---

[108] See, for example, the 'Modifications' section of the Spy Blast EULA, online: <http://www.ftc.gov/os/caselist/0423196/050803exibsad0423196.pdf >.
[109] *PIAC Spyware Survey* (Appendix III) questions 15 and 16,and *Ponemon Study, supra* not 31, at 8.
[110] *Estrange*, *supra* note 100. This English case is infamous for its strict adherence to 'buyer beware.' The Court upheld a clause that was unread by the defendant.
[111] *Tilden, supra* note 90.

embedding terms in an unnecessarily lengthy EULA could be argued to be unreasonable and vitiate acceptance of the contractual terms, even though this analysis contradicts the ratio in *Rudder, Caspi* and *Kanitz*. Finally, the disclosure of spyware behaviour or of bundled spyware could constitute an 'onerous' term.[112] Hence under the rules set out in *Tilden* it is possible that contracts provided by spyware companies are insufficient to achieve the user's assent.

Tilden was raised in the *Kanitz* decision, but Judge Nordheimer distinguished the case due to his belief that the clause in question was not hidden, nor was their any "fine print" (applying the logic from *Rudder* and *Caspi*.) Judge Nordheimer also suggested that the plaintiff's evidence regarding the difficulty in finding the user agreement and amendments was disingenuous. The facts demonstrate that the defendant made many attempts to draw customers' attention to the customer service website, where agreement updates were posted, and the amendment clause was included in the first page of the agreement. In concluding that *Tilden* did not apply, Judge Nordheimer referred specifically to the lack of fine print, but the above factors also played an important role in his analysis. In spyware EULAs the software vendor usually makes no attempt whatsoever to draw users' attention to important clauses or information, hence it remains quite possible, even likely, that the rule from *Tilden* will apply to such spyware cases.

Another option for judges seeking an equitable solution to material disclosures buried within EULAs is to strike the agreement out on public policy grounds. Courts have in the past voided contracts or specific provisions in contracts for public policy reasons.[113] Often these cases involved contracts for immoral or illegal activities that the courts refused to uphold. In spyware cases PIPEDA could be applied in a novel manner to strike down these contracts.

---

[112] The following is an example of a possible 'onerous term' in a spyware contract:

> 9. OTHER SOFTWARE. You allow that 3rd Prty [sic] ad-supported software (adware) will be installed in addition [to] the source file that you are about to install after the Metrix Marketing Group installation procedure. Metrix Marketing Group provides the free distribution of legally distributable software, content and other electronic computer application[s]. We rely on 3rd party ad-supported applications to monetarily support our distribution. The Metrix Marketing Group Inc. shall not be liable to anyone with respect to such third party software. If you wish to remove the associated ad-supported software follow the uninstall links located here: [none provided]
>
> Each 3rd Party adware company has it's [sic] own associated terms and conditions that are also made available to the end-user. The vendor's End User Licence Agreement (EULA) shall govern the use of the software.
>
> For YourSiteBar license agreement go here: http://www.ysbweb.com/terms
>
> For A Better Internets license agreement go here: http://www.abetterinternet.com/policies.htm
>
> For SearchMiracle license agreement go here: http://www.searchmiracle.com/TERMS.htm
>
> For TopConverting license agreement go here: http://www.crazywinnings.com/activex/conditions.php

[113] For example, *Ashmore, Benson, Pease & Co Ltd v. AV Dawson Ltd* [1973] 1 WLR 828 (U.K.), *re Baby M*, 537 A.2d 1227, 109 N.J. 396 (U.S.)

While PIPEDA itself is without sufficient remedy, it is still technically law and breaching the act would be considered "illegal". Hence EULAs that do not meet the requirements of PIPEDA for transferring personal data could be struck down for public policy since their execution is technically illegal.[114] This is another tool that could potentially be employed by the courts to strike down EULAs that are clearly unfair.

Conclusion

It is uncertain whether EULA terms that disclose bundled software or spyware behaviour are binding according to contract law. Additionally, consumer protection legislation will likely only void the contract in extreme cases, as outlined below.

Regardless of whether the user has assented to the EULA and the software download, the only private remedy available to the individual user would be rescission and restitution or possibly trespass to chattels. Damages in these cases would likely be minimal, barring disgorgement or punitive damages, although they could be combined into large class-action suits against spyware companies. Alone they would not be worth the user's time, nor would they sufficiently deter spyware producers. Once established, lack of assent does improve the odds of a Criminal Code conviction, but lack of resources makes it unlikely that police forces would investigate or that the Crown would prosecute.

The scant caselaw regarding 'clickwrap' demonstrates a general lack of jurisprudence on software installation methods. As noted in the spyware jurisprudence section above, the prevalence of settlements in cases regarding spyware to date have also prevented any spyware-specific caselaw from emerging. This may be a case of technology advancing far faster than the common law can adapt, and legislation may therefore be necessary to get the law up to speed. What little caselaw there is has not developed in a manner that is consumer-friendly (for example, *Rudder, Caspi* and *Kanitz*). While the common law could step in to help in the fight against spyware, the process would be slow and uncertain, and lacks strong remedies necessary for cases to come forward. The only opportunity for quick reversal of spyware trends with law appears to be via consumer protection statutes.

Consumer Protection Legislation – Ontario

The Ontario Consumer Protection Act (CPA) contains protections against unfair practices and a set of new regulations dealing specifically with Internet contracts. However there are several hurdles to overcome before consumer protection legislation may apply to spyware downloads.

[114] Ian Kerr "If Left to Their Own Devices" in Michael Geist, ed. *In the Public Interest* (Toronto: Irwin Law, 2005) at 193-196.

Definitions in the CPA

First, the installation must be considered a "consumer transaction", which is defined in the act as an "act or instance of conducting business or other dealings with a consumer."[115] During spyware downloads, users usually 'pay' for desirable software by downloading undesirable software. This seems to fit the description of a consumer transaction, however it is possible that some spyware downloads may not meet this requirement. A policy analyst at the Ministry of Government Services suggested that such a spyware download may not be a consumer transaction, while a compliance manager believed that it likely would be.[116]

Unfair practices

The act prohibits 'unfair practices,' and states that any misleading or deceptive representations are considered 'unfair practices':

> **False, misleading or deceptive representation**
> **14.(1) It is an unfair practice for a person to make a false, misleading or deceptive representation.**

Two examples of false, misleading or deceptive practice are:

> **14.(2) 10. A representation that a service, part, replacement or repair is needed or advisable, if it is not.**
> **14.(2) 14. A representation using exaggeration, innuendo or ambiguity as to a material fact or failing to state a material fact if such use or failure deceives or tends to deceive.**

These sections cover any misleading or deceptive language in EULAs, often prevalent in spyware EULAs, as well as advertising techniques that point out flaws in a user's computer that do not actually exist. This tactic often employs pop-ups or banners that resemble system messages to deceive users and make them respond.[117]

However many spyware companies, particularly the more established, have turned towards more complete disclosure in their EULAs. Users rarely read EULAs, and will almost certainly not read long EULAs.[118] They can therefore

---

[115] *Ontario Consumer Protection Act*, 2002, S.O. 2002, c. 30, Sched. A., at section 1, Online: <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/02c30_e.htm#BK2>. [*Ontario CPA*].
[116] Rob Harper, a policy analyst at the Ministry, said it may not be considered a transaction (phone conversation, July 21, 2005.) [*Harper*]. Vishnu Kangalee, a compliance manager, said it probably is a transaction (phone conversation, August 24, 2005.)
[117] *See* Ben Edelman, "Claria's Misleading Installation Methods - Ezone.com" benedelman.org (April 2005), online: <http://www.benedelman.org/spyware/installations/ezone-claria/details.html#1c>. [*Ezone*].
[118] Nathaniel Good et al. "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (Paper presented to the Symposium on Usable Privacy and Security, July 2005) (New

afford to make full disclosures in clear language, and provided the disclosures are made deep within a lengthy EULA the users will never be aware that the installation includes spyware and will be more likely to consent to the installation.

New Internet agreement regulations

Section 5 of the *Consumer Protection Act, 2002* would be more successful in addressing this problem, if it is applicable:

> **5.(1) If a supplier is required to disclose information under this Act, the disclosure must be clear, comprehensible and prominent.**

The disclosure requirement regulations for Internet contracts contain a requirement for Internet agreements to disclose "a fair and accurate description of the goods or services being sold to the consumer, including any relevant technical specifications."[119]

Section 5 of the CPA could be employed as a tool in actions against spyware companies, since the information must not only be disclosed in a manner that is not misleading, but must also be clear, comprehensible and prominent. However the application of these regulations is conditioned upon a threshold of $50 value of the transaction.

To apply the more restrictive new regulations (potentially the most effective tools in combating spyware,) the value of the transaction must be at least $50. Placing a dollar value on a spyware transaction is extremely difficult. If the replacement value of the software being 'purchased' is the correct gauge, then the transaction is likely worth far less than $50. If the invasion of privacy, irritation, and cost of removal can determine the price, than the transaction could be valued higher. It seems likely that this method of measuring price is too indirect, in which case the requirement will not be met.

Specific to Internet agreements, the Act also states:

> **Manner of disclosure**
> **(3) In addition to the requirements set out in section 5, disclosure under this section shall be accessible and shall be available in a manner that ensures that,**
> **(a) the consumer has accessed the information; and**
> **(b) the consumer is able to retain and print the information.**

The requirement to ensure that the consumer has accessed the information may also catch lengthy and overly complicated EULAs.

York: ACU Press, 2005), online: <http://portal.acm.org/citation.cfm?id=1073001.1073006> [*Good*].

[119] Draft regulation under the *Ontario CPA*, Part IV, Rights and Obligations Respecting Specific Consumer Agreements, ia.2.2.

Additional protections exist in the act for lack of substantial consideration, excessively one-sided agreements and to account for ignorance or inability of the consumer to understand the agreement.[120] These protections could also apply to spyware installation tactics, particularly when the free software is practically worthless or easily available for free elsewhere.

Conclusion

The final hurdle to overcome is motivating the appropriate ministry to take action against spyware companies; otherwise the only remedy available to consumers is the voiding of unfair contracts. It is uncertain if spyware would hit the ministry's radar screen; from informal discussions with a policy analyst it appears that spyware is not considered a candidate for legal actions.[121]

When each of the obstacles is considered, consumer protection legislation is far less capable of dealing with spyware than it appears on first glance. It seems that the new regulations would likely not apply due to the $50 value requirement, although there is an argument to be made for their application. Without the new regulations the CPA will only cover the worst cases of spyware.

Similar consumer legislation exists across the country,[122] and is likely the best way to approach spyware with current law. New York Attorney General Spitzer's recent action against Intermix Media was based in part on state consumer protection legislation and the FTC's actions are almost all based on "unfair" business practices. However, as with most current law, this type of legislation is almost certain to catch the worst cases of fraudulent and deceitful installations, but not the more common incidents of spyware where weak or unclear disclosures are made. Consumer protection legislation has the further drawback of requiring the appropriate ministry to take action against the offenders. For this to occur in Ontario, the Ministry of Government Affairs looks at many factors, including the number of complaints, the dollar value of the transactions, the vulnerability of consumers and the general scope and breadth of the complaint.[123] Nevertheless, such legislation may play a role even now in voiding online contracts that were established through unfair practices.

PIPEDA

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is federal legislation that regulates the collection, use and transfer of

[120] *Ontario CPA*, S.15.(2)(a)-(e)
[121] *Harper, supra* note 108.
[122] Provincial legislation pertaining to internet contracts has been modeled on the 1999 Uniform Electronic Commerce Act (UECA) and the 2001 Internet Sales Contract Harmonization Template (ISCHT.) ie: *Alberta Fair Trading Act*, *Nova Scotia Consumer Protection Act.*
[123] Conversation with Rob Harper at the Ministry of Government Affairs, July 21, 2005.

personal information by businesses and other organizations. Provinces were given the opportunity to pass substantially similar legislation that would take precedence over PIPEDA in the province in question. Only British Columbia, Alberta and Quebec passed such legislation. While PIPEDA does not apply in these jurisdictions, their respective provincial legislation is similar to PIPEDA. PIPEDA offers some redress to victims of privacy violations, but it is only in the form of an investigation by the privacy commissioner, which may be followed by a complaint from the privacy commissioner to the privacy violator.[124]

The most relevant PIPEDA complaint was that of a customer in 2003 who complained that an airline company was violating his privacy rights by refusing his entrance to the airline's website unless he allowed cookies to be installed on his computer. The consumer further complained that the company was tracking browsing habits and stealing personal information without consent through the use of cookies.[125]

The commissioner found that the first complaint was well founded and resolved by the airline discontinuing this practice. The commissioner also found that the second complaint was well-founded and contravened principle 4.3.

This case can be distinguished from spyware cases based on the fact that no EULA at all is presented to a user who receives a cookie, whereas EULAs are often given to users who download spyware (even though they may be misleading or unclear.)

Principle 4.3 of PIPEDA states "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where appropriate." This requirement was clarified in *Englander v. Telus*[126] as 'informed consent'. It is evident that downloading software that collects personal information without disclosing such behaviour is in breach of PIPEDA. However, it is uncertain whether displaying a lengthy EULA that discusses privacy concerns somewhere in the agreement can be considered sufficient to achieve the 'informed consent' of the user. The case above does not help answer this question, but it would seem natural that informed consent regarding privacy concerns requires something more than a reference buried deep within a lengthy EULA. It is highly likely that many of the practices employed by the spyware industry would qualify as a breach of principle 4.3.

While spyware companies frequently violate principle 4.3 of PIPEDA by deceiving users into downloading tracking software without obtaining informed consent, this debate is largely academic since there is little that PIPEDA can do

---

[124] The Public Interest Advocacy Centre, *Consumer Privacy Under PIPEDA: How are we Doing?* (Ottawa: PIAC, 2004), online: <http://www.piac.ca/PIPEDAReviewFinal.pdf>. [*PIPEDA Report*].
[125] Canada, Privacy Commissioner, *Findings fro PIPEDA Case Summary #162*, (Ottawa: Privacy Commisioner, 2005), online: <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_7_e.asp>.
[126] *Englander v. Telus,* 2004 FCA 387.

to prevent these practices. A complaint can be filed and an investigation completed, but the privacy commissioner lacks any strong enforcement mechanism to punish these companies.[127] The successful complaint in the case above has done nothing to prevent the continuing activity of installing cookies on Internet users' computers without consent.

Trespass to chattels

The tort of trespass to chattels could also be applied to sue spyware firms, since software that installs itself unknowingly on to one's computer can be considered interfering with a chattel. To make a successful claim for trespass to chattels the interference must be without consent (unauthorized), and the resulting injury must be sufficiently direct and immediate.[128] The requirement of 'injury,' or damage, seems to be a definite requirement in the American common law, but trespass to chattels according to British law seems to be actionable without proving damage. It is uncertain if damage is necessary in the Canadian context.

In the case of spyware, an argument can be made that the chattel is being interfered with since the software will often bring up irritating pop-up ads, alter system settings and slow down the computer to some extent.[129] The resulting injury, if necessary to found the tort, may be minimal (the malfunctioning of a computer and the time and money spent by the victim to fix the situation,) but it does exist. Since consent to the download can be said to be lacking in many instances of spyware, this tort is may be actionable against spyware. This action was included in Spitzer's claim against Intermix and in all of the class action suits listed above.

However, the law of trespass to chattels in relation to spyware is developing slowly in the U.S. and is so far undeveloped in Canada. Part of the uncertainty in the law is the result of a U.S. decision of the Supreme Court of California regarding trespass to chattels for spam, not spyware, called *Intel* v. *Hamidi*.[130] The court there rejected the "harm" element necessary for the action, which was allegedly occasioned to the Intel system by former employee Hamidi spamming their server with anti-Intel e-mails. The *Hamidi* court also rejected the notion that the user's wasted time was sufficient harm to ground the claim. *Hamidi* has retarded U.S. actions of trespass to chattels for spyware, but some cases continue.[131]

---

[127] *PIPEDA Report, supra* note 116.
[128] John Fleming, *The Law of Torts, 6th ed*. (Sydney: Law Book Co., 1983) at 47.
[129] See "Downloading Software onto Home Computer May Be Trespass to Chattels--Sotelo v. DirectRevenue" Eric Goldman's Technology & Marketing Law Blog, September 01, 2005, online: http://blog.ericgoldman.org/archives/2005/09/downloading_sof.htm , discussing *Kerrins* v. Intermix and several other cases alleging trespass to chattels for spyware infections.
[130] 30 Cal.4th 1342, 71 P.3d 296, 1 Cal.Rptr.3d 32 (1993).
[131] See the court's ruling in the motion to dismiss Kerrins v. Intermix Media Inc., discussed by Eric Goldman (see previous footnote), found at;

It is fair to say that the action of trespass to chattels faces is a long, difficult and uncertain route to controlling spyware that consumers may not in any case wish to wait to see develop, especially if Canadian and U.S. courts follow the reasoning in the *Hamidi* case.

The *Criminal Code*

Section 430 of the Criminal Code creates an offense for anyone who willfully:

> **(a) destroys or damages property;**
> **(b) renders property dangerous, useless, inoperative or ineffective; [or]**
> **(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property;**

This section could certainly be applied to spyware that renders computers useless or interferes with their lawful use because of excessive consumption of processing power or excessive pop-up advertising. However this offense will apply only in the most extreme cases of spyware infections, and 'above ground' spyware companies that could most easily be targeted have in most cases stopped infecting computers on such a massive scale. It is not in their interest to make the computer inoperable – they cannot receive advertising commissions or spy on browsing habits if the computer is rendered useless. The defense of user consent could also be applied. Section 429(2) states:

> **(2) No person shall be convicted of an offence under sections 430 to 446 where he proves that he acted with legal justification or excuse and with colour of right.**

If clicking 'I agree' beside a EULA is considered consent then it is quite possible that this defense will be successful.

Section 184 of the Criminal Code may also cover keyloggers or other devices used to intercept communications:

> **(1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.**
> **(2) Subsection (1) does not apply to**
> **(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;**

Section 342.1 would also cover various spyware related offences:

---

http://blog.ericgoldman.org/archives/kerrinsintermixmotiondismiss.pdf as well as the other cases mentioned by him.

(1) Every one who, fraudulently and without colour of right,
(a) obtains, directly or indirectly, any computer service, [or]
(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted… …any function of a computer system,
is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

The offence of fraud could be applied to fraudulent installation procedures:

380. (1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service, [is guilty of an offence]

These offenses, however, would largely be reserved for the worst spyware offenders, which are inevitably the most difficult to prosecute since they are often small companies located out of jurisdiction. The heavy burden of proof, the frequently complex web of affiliates,[132] the lack of resources among police forces to collect the necessary evidence and the uncertainty in whether the Crown would prosecute lead to the conclusion that the criminal law is likely not the best venue for tackling the spyware problem.

The *Competition Act*

The federal *Competition Act*[133] could also be applied to deceitful installation procedures, much like the Ontario *Consumer Protection Act, 2002*. The *Competition Act* states:

74.01 (1) A person engages in reviewable conduct who, for the purpose of promoting a product or business interest,
(a) makes a representation to the public that is false or misleading in a material respect;

[. . .]

52. (1) No person shall, for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever, knowingly or recklessly make a representation to the public that is false or misleading in a material respect.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC), along with the Center for Democracy and Technology, recently filed a complaint with

[132] Testimony of Ari Schwartz, Associate Director, Center for Democracy and Technology, before The House Committee on Energy and Commerce on "Combating Spyware: H.R. 29, the SPY ACT" January 26, 2005. Tracking spyware producers and holding them accountable for their installation procedures is increasingly difficult due to their complex affiliate programs.
[133] R.S.C. 1985, c. C-34, as am.

the Competition Bureau in early November 2005, alleging infringement of s. 74.01 of the Competition Act. The subject of the complaint, Integrated Search Technologies (IST), allegedly created the impression that users were required to download software to receive pirated serial numbers or MP3s, when in fact IST's software was unnecessary or the products were unavailable regardless of the installation. The company also used Microsoft's security center images to give the impression that Microsoft was sending messages to the user, when in fact it was an animation delivered from the software vendors themselves. The Competition Bureau has yet to act on the complaint.[134]

CIPPIC appears to have avoided pleading s. 52(1) of the *Competition Act* as a basis for its complaint. This is likely because s. 52(1) requires a software publisher to "make a representation". Most spyware, however, relies upon omissions. That is, in "drive-by" downloads – often the worst installations, there are no statements but rather a failure to make a representation where a consumer normally would expect one detailing the software installed and system changes effected.

While penalties in the *Competition Act* may be stricter than those in consumer protection legislation and the Act may be successful in addressing the behaviours listed above, this conduct is once again fairly extreme by spyware standards. Unlike its American counterpart, the FTC Act, the *Competition Act* does not contain provisions outlawing "unfair" behaviour that could be successful against standard spyware installation tactics.[135] This behaviour is covered by consumer protection legislation in Canada. Hence provincial consumer protection acts seem more appropriate to attack the various spyware related activities in Canada. The *Competition Act* would likely only apply to worst-case offenders,

---

[134] CIPPIC "Law Enforcement" *Projects and cases – Spyware*, online: <http://www.cippic.ca/en/projects-cases/spyware/#law-enforcement>.

[135] Of note is a private member's bill presently before the House of Commons. Bill C-299 *An Act to amend the Criminal Code, the Canada Evidence Act and the Competition Act (personal information obtained by fraud)* (Rajotte) (http://www.parl.gc.ca/PDF/39/1/parlbus/chambus/house/bills/private/C-299_1.PDF) would, in part, amend the *Competition Act* to:

> (a) characterize the business of fraudulently obtaining personal information as an illegal trade practice;
> (b) characterize the promotion of a product that is provided by means of fraud, false pretence or fraudulent personation as a false or misleading representation to the public; and
> (c) provide for the recovery of damages from corporations within Canada affiliated with corporations outside Canada that have obtained personal information from third parties in Canada by fraud, false pretence, or personation.

This bill likely is aimed at catching identity theft (pretexting), however, the wording of the bill may be sufficiently wide to catch most spyware in the same manner as the U.S. FTC Act.

and also suffers from a jurisdictional clause that is not well suited to deal with Internet offences.[136]

Children and spyware

Many spyware producers target children's websites in an effort to 'get in the door' of a computer, since children tend to be less thorough then adults in installing software.[137] Since children cannot generally enter into a contract or give consent, any installation completed by a child cannot amount to the consent required to complete a contract. Similar issues arise when one user installs the software without the knowledge or consent of another user. All advertising to children under the age of 13 is prohibited in Quebec according to the Quebec Consumer Protection Act.[138]

Summary

While legal tools are available to fight spyware, their success against obvious cases is far from certain. PIPEDA is without sufficient remedy, criminal provisions and the Competition Act only apply to the worst offenders, and consumer protection legislation only applies to certain activities in which spyware producers sometimes, but not always, engage. Software installations that make misleading or deceptive claims are likely captured by Canadian statutes, but in many cases it is material omissions or buried EULA disclosures during an installation that characterize software as spyware. It is uncertain if such omissions would be considered 'unfair' according to consumer protection legislation, but even if they are, remedies are still weak for consumers.

It is not clear whether the clickwrap EULAs presented to users by many spyware companies are sufficient for users to grant assent. Particular clauses could be voided for public policy or their potential violation of the rule in *Tilden*. On the other hand users have actively clicked 'I agree' with the contract in view, and the courts have upheld lesser actions as demonstrating assent in the past.[139] While claims can be brought against spyware companies with current legislative or common law tools, consumers and public officials seeking to take action against them would benefit greatly from legislation or case law that clarifies this area of the law and details what is actionable and what is not.

---

[136] *Competition Act* (R.S. 1985, c. C-34) at s. 74.03 (2) Where a person referred to in subsection (1) is outside Canada, a representation described in paragraph (1)(a), (b), (c) or (e) is, for the purposes of sections 74.01 and 74.02, deemed to be made to the public by the person who imports into Canada the article, thing or display referred to in that paragraph. [An almost identical clause exists regarding S. 52 at 52(2.1).]

[137] Bob Sullivan "Spyware firms targeting children" *MSNBC* (5 May 2005), online: <http://www.msnbc.msn.com/id/7735192//>. [*Sullivan*].

[138] Quebec Consumer Protection Act (R.S.Q. c. P-40.1) at s. 248.

[139] *Kanitz*, *supra* note 99.

JURISDICTIONAL ISSUES

International jurisdictions

A significant issue when dealing with spyware regulation, similar to many Internet legal problems, is the question of jurisdiction. Using the conventional Zippo 'passive versus active' test[140] as well as the more recent effects-based or targeting tests,[141] spyware producers should be liable in any jurisdiction in which their software is downloaded. Once these companies have entered contracts with individuals from a jurisdiction, they have indicated an active attempt to do business there. They have also in many cases caused harm in that jurisdiction by uploading malicious or unwanted software onto the user's computer. Barring some kind of evident action that demonstrates that they are not soliciting customers from particular jurisdictions, claims could potentially be filed against them in any jurisdiction in which their software has been downloaded.

While these tests for jurisdiction may function well for American authorities taking action against spyware companies located in other US states or in Canada, and for Canadians seeking jurisdiction over American companies, their application becomes much more uncertain in other jurisdictions. Even if tough anti-spyware legislation is enforced successfully in North America, underground companies can continue their practices in offshore jurisdictions that are beyond the reach of US or Canadian authorities. The infamous Cool Web Search, one of the most prevalent and nefarious spyware companies,[142] is rumoured to be located in Bermuda.[143] The unfortunate consequence is that any complete spyware solution will likely require extensive international cooperation.

Despite this obvious flaw in any attempt to regulate spyware producers, it should not be used as an excuse for inaction. As discussed at various points throughout this paper, the spyware industry will almost always contain an underground element that will be more difficult to regulate. Meanwhile 'above ground' companies, many of which are located in the United States and are not capable of moving anywhere quickly, can be relatively easily reformed to meet certain standards set by lawmakers. Additionally, the most recent spyware report from Webroot concludes that 31% of all sites using exploits to download code to users' machines are hosted in the US.[144] In any case, the effort to regulate spyware should not be seen as a failure if it does not result in wiping the Internet clean of all malicious software. Instead such efforts should be viewed in terms of

---

[140] *Zippo Mfg. Co. v. Zippo Dot Com*, *Inc*. 952 F. Supp. 1119 (W.D. Pa. 1997).
[141] *See* Michael Geist *Internet Law in Canada, 2nd Edition*, (Captus Press, Toronto: 2001) at 64 – 72.
[142] *Webroot Q1*, *supra* note 43 at 7.
[143] *Download.com Antispyware Workshop,* (3 May 2005), Session II, 43:10. (Esther Dyson speaking.) MP3 of workshop audio available at Release1-0.com and on file at PIAC.
[144] *Webroot Q3*, *supra* note 47 at 27.

establishing standards and transparency in the software industry to grant the public more knowledge and control over what their software does and which types of software they want on their computer.

Canadian constitutional law: federal or provincial jurisdiction?

If legislation is applied to combat the spread of spyware, it must be decided whether such legislation is within the provincial or federal jurisdiction. The Canadian *Constitution Act, 1867* establishes jurisdictions within which either the provincial legislatures or the federal parliament have the authority to govern. It is somewhat uncertain in which jurisdiction the issue of software installation regulation would fall, but possible that the federal government could claim jurisdiction through the trade and commerce power.

The trade and commerce power

The *Constitution Act, 1867* gives parliament jurisdiction over the "regulation of trade and commerce" (S. 91(2)) while the provincial legislatures have jurisdiction over "property and civil rights in the province" (S.92(13)).[145] These two powers frequently come into conflict since trade and commerce often, if not always, involve the trading of property and rights.[146]

There have been two methods outlined by the courts through which the federal government may justify its legislation under the trade and commerce jurisdiction. First, it may do so by establishing that the legislation's purpose is to regulate inter-provincial or international trade and commerce. Second, it may establish that the legislation is 'general' legislation that is not aimed at any particular industry but at trade and commerce as a whole.

The stronger argument for federal jurisdiction over software downloads lies in the inter-provincial or international trade justification. For Canadians, downloads usually occur across borders, and according to Peter Hogg, "There is no doubt that the federal trade and commerce power will authorize the regulation or prohibition of the importation of goods into Canada."[147] Federal legislation that covered only inter-provincial transactions was always upheld in the past, and Supreme Court decisions from 1959 on upheld such legislation even though it affected intra-provincial transactions provided that the impact was incidental to the main object of regulation.[148] While Hogg remains uncertain about the ability of the trade and commerce power to uphold federal jurisdiction over markets with only some inter-provincial trade flows, considering the magnitude of software downloads that occur across provincial and international boundaries it is highly

---

[145] *Constitution Act*, 1867. U.K., 30 & 31 Victoria, c. 3. [*Constitution Act*]
[146] Hogg, Peter. *Constitutional Law of Canada, 2nd ed*. (1985: Carswell, Toronto.) at pg. 440 [*Hogg*]
[147] *Ibid*, at 443.
[148] *R . v. Klassen,* (1959) 20 D.L.R. (2d) 406 (Man. C.A.), *Caloil v. A-G Can*., [1971] S.C.R. 543.

likely that the federal government will be capable of exerting jurisdiction over the practice of software downloading.

The alternative justification is the 'general' trade and commerce power. *Citizens' Insurance Co. v. Parsons (Parsons)*[149] gave an indication of the judicial interpretation of this power. In that case a provincial statute aimed to regulate fire insurance policies. The law was upheld on the grounds that the federal government had jurisdiction only over general trade and commerce, but the provincial governments maintained the right to legislate with relation to specific industries. This rule from *Parsons* would indicate that the federal government does not have jurisdiction to legislate purely in relation to the trade of computer software under the 'general' trade and commerce power. Additional analysis based on *General Motors of Canada Ltd v. City National Leasing*[150] indicates that this conclusion is likely correct. In that case the Court laid down five criteria for establishing when the general power applies.[151] These are:

1. The impugned legislation must be part of a general regulatory scheme;
2. The scheme must be monitored by the continuing oversight of a regulatory agency;
3. The legislation must be concerned with trade as a whole rather than with a particular industry;
4. The legislation should be of a nature that the provinces jointly or severally would be constitutionally incapable of enacting; and
5. The failure to include one or more provinces or localities in a legislative scheme would jeopardize the successful operation of the scheme in other parts of the country.

While these are merely criteria and not a five-step test, qualifying federal anti-spyware legislation under the 'general' justification could be difficult given the third criterion. However, when spyware affects even "mainstream" applications such as Sony BMG's rootkit fiasco, an argument can be made that the software industry as a whole is the target, not simply adware vendors.

The peace, order and good government power

The peace, order and good government provision may also place spyware in the federal government's jurisdiction. S. 91 of the *Constitution Act, 1867* allows the federal government to "make laws for the peace, order, and good government of Canada…"[152] Thus any residual powers not enumerated in the list of powers are meant to reside in the federal government's jurisdiction. One branch of interpretation of this section has come to conclude that any area of

[149] *Citizens' Insurance Co. v. Parsons,* (1881) 7 App. Cas. 96. (JCPC).
[150] *General Motors of Canada Ltd v. City National Leasing,* [1989] 1 S.C.R. 641.
[151] Murray Long and Suzanne Morin, *The Canadian Privacy Law Handbook*, (Toronto: Centrum Information and Conferencing, 2000) at 48.
[152] *Constitution Act*, *supra* note 132.

'national concern' is under federal jurisdiction.[153] The 'national concern' has been defined in several ways, but the most successful method has been the "provincial inability test", which defines an issue as a national concern if the provinces would be unable to take care of the problem on their own.[154] This definition may apply to spyware, since single provinces legislating against spyware alone would be far less effective, and perhaps useless, compared to a national law to combat the problem.

Hence the trade and commerce extra-provincial trade branch or the peace, order and good government power could be applied to establish federal jurisdiction over the problem of spyware. It is likely that one or both of these justifications would be successful. In any event, the provinces may welcome federal jurisdiction in the area since a uniform national law seems logical to combat the problem.

Software installations would also fall into the category of property and civil rights under 92(13) of provincial jurisdiction. They may therefore constitute a "double aspect" issue, meaning that both the provincial and federal governments may legislate in the area.[155] If this is the case, parliament could offer provinces the opportunity to pass substantially similar legislation. Federal legislation would have paramountcy over provincial laws on the issue if conflict arose between the two regimes.[156]

The PIPEDA-*model Approach*

Finally, however, it should be underlined that spyware or malware presents a completely novel problem to the Canadian federation, much as it has with privacy under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). With privacy, the constitutional solution proposed was a compromise or 'carrot and stick' approach with the federal government leading the way. The PIPEDA-model provides for the federal government to pass a law under federal jurisdiction that may treanch on provincial jurisdiction but allow a province to pass a law which is "substantially similar", in order to achieve a standard baseline of law in a developing area. Practically speaking, only a uniform legal approach can hope to control spyware throughout Canada. The PIPEDA-model has proven effective in achieving a baseline of privacy protection in Canada and could similarly 'cut the Gordian knot' of jurisdictional wrangling in the equally novel area of regulating spyware or malware.

[153] Hogg, *supra* note 133 at 375.
[154] *Ibid,* at 380
[155] See for example, *Multiple Access Ltd. v. McCutcheon*, [1982] 2 SCR 161.
[156] *Bank of Montreal v. Hall*, [1990] 1 SCR.

SUGGESTED REACTIONS

The spyware experience has demonstrated that where money can be made, individuals and corporations will take advantage of poorly defined law to wrestle control of personal computers away from the users who own them. The most important signal that government can send to this market is that the right to control a personal computer rests solely with the user of that computer, and this control cannot be undermined except in a clear and fair manner to the computer user. Government should also indicate that those who hide behind affiliate networks to avoid liability for trampling on users' rights cannot do so with impunity.

In this light, trespass to chattels or consumer protection violations should certainly be explored as causes of action against spyware purveyors for their actions or those of their affiliates. However, single claims against spyware companies provide very little disincentive to bad actors. Hence legislation may be advisable to create penalties that are sufficient to make companies pay attention. This legislation can be aimed at defining the term "unauthorized" as it relates to software installations. Users and software publishers need clearer guidelines on what type of software behaviour must be disclosed, and how these disclosures should be made.

Enforcing current law

The most pressing concern for the Canadian government regarding spyware should be to begin enforcing current laws against spyware vendors and affiliates. These laws will not cover the full spectrum of spyware behaviour, but will almost certainly catch extreme cases. While the FTC and state Attorneys-General may have been slow to begin tackling the spyware problem in the United States, in Canada no spyware cases have been pursued by any government or private actor, with the exception of the CIPPIC/CDT complaint against IST filed with the Competition Bureau/FTC. This is distressing, and the lack of deterrence against spyware behaviour is may be partly responsible for several spyware operations opening in major Canadian cities.[157]

A significant obstacle to active enforcement is the uncertainty surrounding which department is responsible. Police forces are short on resources and are devoting their energies to more harmful Internet crime, such as child pornography. While some investigations have been conducted into modem hijacking, police forces are unlikely to investigate spyware because it is unlikely to be prosecuted under criminal law.[158] While a spyware complaint has been

[157] For example, Integrated Search Technologies in Montreal (see http://www.cippic.ca/en/news/documents/Affidavit-IST.pdf) and Mirar (Toronto).
[158] From a conversation with Barry Elliot, Staff Sargeant, Ontario Provincial Police, and creator of Phonebusters, an anti-fraud call center. August 17, 2005.

filed with the Competition Bureau, an investigation has not yet been initiated at the time of writing. Consumer protection ministries, such as the Ministry of Government Services in Ontario, are also not currently pursuing spyware.[159] There is no equivalent to the Federal Trade Commission (FTC) in Canada, and the Canadian constitution prevents Attorneys-General from conducting independent investigations. At the moment, it seems that every potential enforcer believes spyware may be in the jurisdiction of another department, impeding progress. More formal and informal cooperation would likely assist in clarifying responsibilities of each government level and government department.

The problem of who is responsible is aggravated by the technical nature of the behaviour to be regulated. Outside experts, specialized equipment and training may be required to monitor software downloads and to record them. In crafting a response to the problem of spyware, the federal government should first identify which department is responsible for enforcement of current and future laws that prohibit spyware behaviour, and devote resources to it. An expansion of an existing department into an organization more closely resembling the FTC, with a clear mandate to investigate spyware cases, may be advisable.

Future regulation

Given the current legal environment, a legislative response may be necessary to fully address the spyware problem. Despite the jurisdictional problems inherent in any Internet regulation, there are strong reasons why spyware requires regulatory action. First, while Canadian laws will catch the worst offenders, there are still many installation tactics that fall into a gray area or may not be illegal at all, despite the fact that studies show many people who have such software installed do not know that it is installed.[160] Even if current laws were applicable to all spyware, remedies available through private actions are likely to be insufficient both to compensate victims and deter perpetrators. Second, as mentioned earlier, the spyware industry is stratified into above ground and underground companies. While the underground will always be elusive and difficult to regulate, the practices of the established above ground companies can certainly be improved. Third, other large, established and previously trusted companies have recently started engaging in spyware tactics in order to either revive failing business models or simply to raise revenues.[161]

---

[159] Conversation with Rob Harper at the Ministry of Government Affairs, July 21, 2005

[160] *Ponemon Study*, *supra* at 11-12.

[161] Ask Jeeves is the most glaring of these examples. Popular lyrics, torrents and kids sites have been inundated with banner ads for 'smiley faces', 'cursor enhancements' and other software. These programs are developed by a company recently acquired by Ask Jeeves (Fun Web Products,) and install with minimal disclosure. The use of cartoon characters in marketing these products also indicates that children would be particularly likely to download them. Users discover after installation that an unbranded Ask Jeeves toolbar has also been installed. This toolbar returns sponsored search results that are virtually indistinguishable from legitimate search results. See Ben Edelman, "Ask Jeeves Toolbar Installs via Banner Ads at Kids Sites"

These accusations have been refuted by the companies involved, but strong evidence exists of surreptitious downloads and bundling without consent. Despite public outcry, these behaviours continue to occur. This unsettling trend demonstrates a lack of sufficient deterrence from engaging in these activities. The uncertain legal environment invites abuses. A regulatory reaction may be necessary not only to regulate the behaviour of well-known spyware companies, but also to deter other companies from entering the market. This regulation will be most effective if it targets the installation procedure and clarifies the rules of installing potentially unwanted software.

Aside from installation procedures, there are several behaviours that should be considered when developing an effective response to the spyware problem. These include reining in the affiliate networks by disabling the 'our affiliates did it' excuse, and addressing the targeting of children to obtain installations. Advertisers should also be scrutinized for their role in offering revenue to spyware companies. Their lack of control over where their ads are shown, and by whom, has been crucial in building a business model that harms computer users. International cooperation must also inevitably accompany any attempts to regulate spyware.

Regulating the installation process

Since spyware has no straightforward definition, simply outlawing 'spyware' cannot solve the problem. There are few substantive characteristics that separate spyware from legitimate software. As outlined in the latest documents released by the Anti-Spyware Coalition, every software function executed by spyware (except possibly the lack of an uninstall function) could have legitimate purposes in certain circumstances.[162] For example keystroke loggers, considered some of the most malicious spyware when installed surreptitiously, are employed by software editing programs and other legitimate software.[163] Given these factors, the thrust of regulatory efforts targeting spyware should be directed at the procedure through which the software becomes installed on users' computers, not at the software itself. The anti-spyware bills currently before the US Congress largely fail to address this issue properly.

---

benedelman.org (9 May 2005), online: <http://www.benedelman.org/spyware/installations/askjeeves-banner/>.
Controversy has also surrounded Dell's bundling of these toolbars with Internet Explorer in Dell computers. *See* John Leyden "Dell Rejects Spyware Charges" *The Register* (15 July 2005), online: <http://www.theregister.co.uk/2005/07/15/dell_my_way_controversy/>.
The fact that Ask Jeeves does not brand these products with its corporate name or logo is particularly suspicious – the only way to discover the company is often by reading the EULA or to find copyright notices on related websites.

[162] *ASC Definition Documents*, *supra*, at 3, "Examples of Spyware and Potentially Unwanted Technologies".

[163] For example, EditPlus 2 includes a keystroke logger that can be enabled by the user.

The most obvious way to address a problem with these limitations is to set the rules of installation for potentially unwanted software so that users are given more obvious, clear notice of the potentially unwanted functionality. This is a two-step process. First, behaviours must be identified that characterize potentially unwanted software. Then disclosure requirements for each of those behaviours can be established. If the software displays a listed behaviour and has not met the disclosure requirements, then it has not achieved the user's consent to the download. A private right of action with statutory damages could then be created to give users an incentive to punish companies that do not meet the disclosure requirements, while providing a legitimate deterrent to companies who engage in poor disclosure practices.

An alternative to specific disclosures for each potentially unwanted behaviour is legislating a higher threshold of consent for software installations. This consent standard may be required to be even more clear than an "informed consent" standard (which theoretically could be proved by the prominent display of an easy to understand EULA). A higher level of consent which required the positive manifestation of user consent and which presented the installation to the user in an objectively fair manner, might be the only form of consent that would stop spyware operators from 'gaming the install process". Such a "fair and obvious" consent standard could be legislated; fairness is required in provincial consumer protection statutes; the U.S. FTC Act mandates the inverse of the proposition, prohibiting 'unfair and deceptive' practices. Requiring even higher consent than has been applied in PIPEDA and in the *Competition Act*, thus far, may seem harsh However, this proposal has the advantage of simplicity over more complex disclosure requirements, increases consumer control and gives a real prospect of enforcement, as the evidentiary burden to show a software installation was "fair and obvious" to the consumer would be effectively shifted from the consumer to the company.

While the majority of the regulatory effort must be aimed at the installation process, there is one substantive behaviour that can also be targeted: the uninstall function. Most spyware applications lack uninstall functions altogether, have overly complex procedures to follow, or create pop-up ads during the "uninstall" procedure. These practices are highly irritating to users, but may not be illegal unless they are characterized as 'unfair' or 'deceptive' practices by present consumer protection or competition legislation. Hence malfunctioning, non-existent or overly complex uninstall procedures could be prohibited outright.

What is potentially unwanted software?

Certain software behaviours common to spyware applications limit the user's control over the software in question and their computer more generally. The presence of *any* of the following behaviours (not including inadequate consent, which can make any software installation unwanted) should be circumstantial evidence towards establishing the software as unwanted.

The software:

1. Transmits information about the user to external computers automatically.
2. Does not allow the user to control when the software runs.
3. Is supported by advertising (the method of advertising, such as pop-ups or sponsored search results, should be disclosed.)
4. Changes browser or system settings automatically.
5. Is bundled with other software that the user did not opt in to receive.
6. Hides itself by not reporting its presence to the operating system.
7. Updates itself without consulting the user.
8. Has a non-standard uninstall procedure, or no uninstall procedure.

This list is preliminary and can be edited to catch as much unwanted activity as possible while excluding as much legitimate software as possible.[164] The list could be included as a regulation attached to an anti-spyware act in order to facilitate customization of the legislation.

Will additional notice work?

Critics of proposed spyware regulation argue that additional notice will not affect users' behaviour when downloading software.[165] There has been limited research into the topic, and only one significant study has specifically addressed the relationship between notice variance and user behaviour.[166] It has been used both by those who argue that stronger disclosures will affect user behaviour[167] and those who argue the opposing view.[168] The study essentially concludes that, "While notice is important, notice alone may not have a strong effect on users' decision[s] to install an application."[169] This study was conducted by offering participants several programs for download, each of which had three possible installation procedures. The study recorded which programs, with which installation procedures, were downloaded by the participants. One installation procedure only showed the EULA, one showed the EULA and a Microsoft warning dialogue box, and one showed the EULA in addition to a 'short notice' that attempts to sum up important features of the software.

---

[164] The Anti-Spyware Coalition has published a very detailed list of suspect behaviours in its document "ASC Risk Model Description - Anti-Spyware Coalition Risk Model Description" Online: http://www.antispywarecoalition.org/documents/RiskModelDescription.htm These "risk factors" could be used to augment the above list, after study.

[165] Eric Goldman "Study on User Consent and Spyware"*ericgoldman.org* (8 July 2005), online: <http://blog.ericgoldman.org/archives/2005/07/study_on_user_c.htm>. [*Goldman*].

[166] *Good*, *supra* note 110.

[167] Eric Howes "Muddy Data, Vague Notice, & the Swamp of User Consent" *spywarewarrior.com* (14 July 2005), online: <http://www.spywarewarrior.com/elh/muddy_data.htm>.

[168] *Goldman*, *supra* note 150.

[169] *Good*, *supra* note 110 at 9.

Despite the study's conclusion, there is evidence to support the belief that additional notice affects user behaviour. For example, it has been reported that since WhenU began including more thorough disclosures in their recent installations, their installation rates have dropped by 50%.[170] 72% of users surveyed by the Ponemon Institute stated that they would be more likely to read EULAs if they were easier to understand, and 65% stated they would be more likely to read them if a shorter version were available.[171] Providing disclosures of potentially unwanted features could serve as a shorter EULA. 56% of those surveyed by PIAC also stated that they would be more likely to read EULAs if they were shorter and clearer, and 31% said they would be more likely to do so if the main points were summarized at the beginning of the installation.[172] Another recent study concluded that 90% of Internet users have altered their behaviour online because of the threat of spyware.[173] All of these numbers support the idea that consumer education combined with improved, standardized notice could lead to changes in user behaviour.

There are also several drawbacks to the notice and spyware study. First, the sample size is very small – only 31 individuals. Second, no user interaction other than clicking 'next' was required to bypass notice screens, except for the Google toolbar installation.[174] If the user is forced to, for example, click a checkbox before continuing the installation, the user would likely be more conscious of the disclosure being made.[175] Furthermore, the 'short notice' example provided in the study spends almost three-quarters of the display window discussing information collection and use, and only the bottom quarter on equally important, if not more important, disclosures, such as how many programs are being installed, whether pop-up advertising will occur, and whether the program will automatically update or add new programs without consent.[176] While spyware earned its name from surreptitious information collection, this is not necessarily the most important disclosure to be made.

Until more research is completed, whether improved notice will affect user knowledge and behaviour remains uncertain. This uncertainty should not prevent regulation. At a certain point the user will have to take responsibility for ignoring important disclosures, but the bar must be set high enough to protect the public: disclosures of potentially unwanted behaviour must be clear and prominent. At the moment this bar is unreasonably low.

---

[170] *Olsen*, *supra* note 17.
[171] *Ponemon Study*, *supra* note 31 at 9.
[172] *See PIAC Survey*, (appendix III.)
[173] *Pew*, *supra* note 40.
[174] The authors of the study would not provide PIAC with the statistics on how many users elected the limited version of the Google toolbar, which turns off the 'spying' functionality. If many of those who installed the toolbar elected the limited version, this would support the conclusion that additional notice is effective.
[175] *See* Google toolbar disclosure, Appendix II.
[176] *Good*, *supra* note 110, at 5, figure 3.

What kind of notice should be given?

For any potentially unwanted behaviours, specific disclosures separate from the EULA should be given to the user to obtain the user's consent to the behaviour. Such notice must be easy to understand and must be capable of being absorbed quickly by the user. Ideally it will also prevent the user from continually clicking 'next' to complete the installation quickly.

A good example of how such regulations could be structured was proposed by Simson Garfinkel in his comments to the FTC regarding spyware in 2004 (See Appendix II.) Mr. Garfinkel's idea was to develop a standardized labeling system for each software function that was potentially unwanted. Although his list of potentially unwanted behaviours is not identical to that listed above, simple, standardized disclosures such as those proposed by Mr. Garfinkel are an ideal method of communicating potentially unwanted software behaviour quickly to users.

However, as demonstrated by the study described above, notice alone may not be enough for users to gain knowledge of the suspect behaviours of the software in question. Many computer users get into the habit of continually clicking the 'next' buttons to install software quickly, ignoring any notices provided.[177] This practice can be counterbalanced by requiring some user interaction other than simply clicking 'next' or 'I agree' to bypass the additional disclosures. This format of consent can be referred to as 'opt in' in certain circumstances, if users must change the default selection to agree to the installation. Spyware companies frequently use 'opt out' consent by leaving the installation option selected by default, thereby taking advantage of users' propensity to continually click 'next' during the installation process without reading notices. Distinctions between these types of consent could be drawn in legislation to ensure a high level of consent.

Scrupulous software companies frequently require such additional input from the user by requiring a check box to be selected and leaving it unchecked by default. The Google toolbar installation has a similar feature with a radio button (see Appendix II). These features could easily be incorporated into the 'additional disclosure' installation screen, and they are a logical accompaniment to additional disclosures. Since additional disclosures are presumably more important than information in the EULA, they should require more than simply clicking an 'I agree' button to demonstrate that the user has consented to the potentially unwanted features.

Consumer education

Consumer education is certainly a critical aspect of designing a solution to the spyware problem. Consumer education can play an important role in

[177] *Supra* note 29.

improving the correlation between notice and user behaviour. If the importance of extra-EULA disclosures is impressed upon Internet users, they are more likely to be read. The recent study by Pew Internet demonstrates that consumer education can play a significant role in affecting Internet user behaviour.

Several key messages can also be sent to users to prevent spyware installations. These are highlighted by several groups, including the Anti-Spyware Coallition. The most important are likely to be:

- Only download from websites you trust.
- Update your operating system and security software regularly.
- Install a trusted anti-spyware solution.

Consumers can also be educated on anti-spyware software to ensure that legitimate anti-spyware software is used, rather than fraudulent or weak anti-spyware software, which is prevalent on the Internet.

Will the software industry support software installation regulation?

The software industry has so far demonstrated reluctance with respect to new legislation on spyware. In their comments to Congress, Microsoft asked legislators to ensure that proposed legislation did not unnecessarily burden legitimate software vendors.[178] Google has also demonstrated concern that spyware legislation may unnecessarily hamper innovation. The FTC echoed these concerns in 2004, putting up an almost ideological free-market resistance to any proposed legislation when questioned by Congress.[179]

If spyware legislation is well drafted, legitimate software vendors should not be overly concerned about the regulation of installation practices. First, the large majority of legitimate software does not perform the potentially unwanted software behaviours listed above. For example, while many applications contact external servers to find updates, they also ask the user before installing these updates. Only unauthorized updates would be caught as potentially unwanted behaviour. Similarly, if software offers users the ability to opt in to installing additional software or running the software on startup, it would not require additional disclosures.

The cost of improved disclosures regarding potentially unwanted behaviours is also minimal, particularly when compared to the cost of building

---

[178] U.S., Hearing on *"Combating Spyware: H.R. 29, the 'SPY ACT'", Oral Testimony Before the United States House of Representatives Committee on Energy and Commerce*, 109th Congress, (2005) (Ira Rubenstein), online: <http://www.microsoft.com/presspass/exec/irar/01-26-05Spyware_Oral.mspx>. [*Rubenstein*].

[179] "Ubiquitous Spyware Propels New Bills, Drowns Out FTC's Plea for Self-Regulation" *BNA Electronic Commerce and Law Report.* Volume 9 Number 18, at 418.
For more FTC commissioner opinions on spyware regulation, see "Cato Panel Criticizes Spyware Bills" Tech Law Journal (5 November 2005), online: <http://www.techlawjournal.com/topstories/2004/20041105.asp>.

software. Moreover, legitimate software vendors should not fear additional disclosures because their software is desirable – only those companies whose software has unwanted functions or is bundled with unwanted software should be unwilling to make clear disclosures.

Legislation can be drafted in a way to ensure that legitimate software vendors are either not subject to regulations or can easily comply with them. Enforcement rules can also be established where companies are given two strikes before the full cost of an infraction is levied upon them, and public documents can be made available so that compliance can be achieved easily, without excessive legal costs.

Concerns have also been raised that disclosure requirements would force large software packages like an operating systems to make inordinate numbers of disclosures to cover all the software in their packages. These concerns could be addressed by maintaining an exemption for operating systems, which seem to be the only software packages that require very large numbers of programs to be installed.

The prospect of lagging industry support is real and should not be taken lightly. Legitimate software vendors may oppose new regulations because they have done nothing to deserve them. Their position is likely to be, quite understandably, that the spyware vendors have caused the problems, and they should be the ones who should alter their behaviour. Unfortunately this seems to be another case where a few bad actors have ruined the game for everyone else, and rules must be introduced across the board as a result.

Higher consent threshold

An alternative to specific disclosure requirements in the installation process would be a higher threshold of consent for software installations than mere contractual consent. The bargaining positions of the user when accepting a EULA is obviously very low – the agreement is always a standard form, take it or leave it contract. PIPEDA currently uses the level of "knowledge and consent" for the transfer of personal data, while provisions in the *Competition Act* use "fair consent", a term that is being further defined through caselaw. A provision requiring stronger consent would give judges a powerful tool to punish unscrupulous software vendors that employ unfair installation practices.

The advantage of such a provision is undoubtedly its simplicity. A single line added to the Competition Act could suffice. However it is also a very blunt tool, and is dependant on the judiciary to apply in the spyware context. Such a provision would also create more uncertainty for software vendors, since it relies on judicial interpretation to create clear law. Nevertheless, it could be an effective first step in bringing some control over spyware, to be followed with a clearer statutory regime.

Other regulatory concerns

The "our affiliates did it" excuse

As outlined in the description of the adware business model above, affiliate networks are perhaps the single greatest factor contributing to non-consensual installations. Spyware companies reserve a convenient excuse for occasions when their software is caught installing without consent: these installations were performed by the company's affiliates and not the company itself. Hence the company is not responsible for the poor installation procedure. The company then, in some instances, may punish or end their relationship with the rogue affiliate and claim to have solved the problem.

This excuse is artificial. Any software that is installed through affiliates is almost always designed to 'call home' to the original software vendor as soon as an installation occurs.[180] This practice is necessary to credit the affiliate with the download. Additionally most spyware is designed to automatically update itself by contacting the original vendor at various intervals. These practices demonstrate clearly that spyware vendors retain control, or at least can retain control, over their software during the installation process. If they so desired, they could require the software to make disclosures or display a EULA before the installation occurs.

This point was made clear when, in June of 2005, 180solutions announced that it would send a notice to every computer with 180's software installed to notify users of the software's presence and its function.[181] Any proposed legislation or regulation should address the insufficiency of the "our affiliates did it" defense in order to force software companies to retain control of the installation process and to restrict the practice of maintaining absurdly large affiliate networks with pay-per-install incentives.

Spyware has become prevalent largely because there is lots of advertising money behind it and very little accountability. The advertisers use brokers who purchase impressions from adware companies, then the adware companies farm out their installations to affiliates. When a non-consensual installation occurs everyone along the chain pleads ignorance and blames the affiliates, but affiliates are often located in other jurisdictions or are judgment-proof and can provide no remedies to users. Liability must rise up this chain of agents if constructive regulation is to take place.

---

[180] *Howes*, *supra* note 13.

[181] John Cook "You may have this adware hidden on your computer" *Seattle Post-Intelligencer* (28 June 2005), online: <http://seattlepi.nwsource.com/business/230328_180solutions28.html>.

Targeting children

In some cases spyware companies specifically target children to obtain installations, presumably because children are less cautious when downloading software, are more likely to be interested in certain types of software and are more susceptible to certain advertising campaigns. In the summer of 2005 Symantec researchers found that more unwanted software was delivered via kids' sites than any other type of website on the Internet.[182] While not a focus of this report, this is a serious trend that should be addressed in a regulatory response to spyware.

In perhaps the most obvious of these cases, Claria was discovered advertising clock synchronization software on a children's video game site. A banner ad designed to appear as a system message alerted the user that their system clock may be inaccurate. When this banner was clicked a highly misleading installation process was initiated.[183] When confronted with this installation, Jeff McFadden, Claria's CEO, responded: "Online gaming sites on the internet, the average age of people who visit those sites is 29."[184] This comment was made despite the fact that the site in question (ezone.com) has since stratified their site into an area for children under 13 and an area for older children, and the site is guided by a cartoon character named Lenny Loosejocks. The site's privacy policy also claimed that the site was suitable for children.[185] There was little doubt that this site was marketed to and frequented by children when Claria posted its deceptive advertisement.

Ask Jeeves, through its subsidiary Fun Web Products, has also likely been targeting children in recent months with smiley face software and cursor enhancements. Both of these products had highly sub-standard installation procedures when tested in the summer of 2005, and install MyWay search toolbars that return sponsored search results that are very difficult to distinguish from legitimate search results. They are also marketed with cartoon characters that sometimes have nothing to do with the software.

Limitation of or outright prohibition of targeting potentially unwanted software at children may be difficult to regulate but should certainly be attempted when considering a regulatory response to spyware.

---

[182] *Sullivan*, *supra* note 124.
[183] *Ezone*, *supra* note 109.
[184] *Download.com Antispyware Workshop,* (3 May 2005), Session II, 1:06:10 – 1:06:30. MP3 of workshop audio available at Release1-0.com and on file at PIAC.
[185] *Ezone*, *supra* note 109.

International cooperation

In the long term, successful anti-spyware measures will be impossible without international cooperation. While established companies' in nearby jurisdictions can be regulated with relative ease, smaller outfits will move to jurisdictions where the law is as friendly as possible to their activities. In response to this trend, the FTC this year proposed the US SAFE WEB Act, aimed at improving international cooperation in fighting online fraud, spam and spyware.[186] Such attempts at international cooperation with foreign consumer protection groups should be welcomed as the first steps towards a full solution to harmful Internet practices. Any eventual Canadian federal legislation on spyware should specifically empower the agency charged with spyware enforcement to cooperate with foreign counterparts.

Responsible advertisers

A complimentary approach to regulating the spyware industry is to require more due diligence on the part of advertisers to ensure that they are not providing revenue to spyware companies. The original source of revenue for most spyware, as highlighted in the business model section, comes from users clicking on pop-ups or other advertising. The online advertising industry is a complex web of affiliates, but advertisers could likely do much more to ensure that known spyware companies do not display their ads. A rule similar to the 'know your client' rule for financial advisors could be applied to advertising companies to ensure that they have more control and knowledge over how their ads are displayed. These practices could potentially be implemented as industry self-regulation.

Companies who seek advertising from large online advertising companies could also do more to ensure that the advertisers are held responsible for where their ads are displayed. The customers may be in a powerful position to affect industry reform if they decide that the issue is worth pushing.

If successfully implemented, regulation of the advertising companies could be highly effective. The regulation unfortunately begs the question "What is a spyware company?" That question would have to be grappled with and would likely lead to contradictory opinions.

Industry self-regulation

Despite the rationale for regulating the software installation process, it is possible that the software industry will oppose such steps due to a general

[186] The Federal Trade Commission, *The US SAFE WEB Act, A legislative recommendation to congress*, (Washington: Federal Trade Commission, 2005), online: <http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf>.

feeling that legitimate software vendors should not have to be regulated because of the actions of rogue spyware companies and affiliates. While regulation may not affect legitimate software vendors to a great extent, fears of unintended liability and higher legal costs will likely linger. Spyware and adware vendors have continually promised industry self-regulation in the past but non-consensual installations continue to occur due to the incentive scheme in the market. As highlighted above, users are not consumers in this market, they are the product, so there is no incentive for companies to keep computer users happy. Thus the regulation of installation procedures should remain in the hands of government.

However, there is much that the industry can do to aid the fight against spyware. Many of the disclosure practices proposed above and demonstrated in Appendix I below can be accepted as industry best practices and implemented before legislation comes into force, making compliance far simpler. A good rule for legitimate software vendors would be to always err on the side of complete disclosure. A strong software application with desirable features should have nothing to fear from disclosing all of its functionality, including any potentially unwanted behaviour. This practice will improve public confidence in software downloads.

Many strong suggestions were made in a staff report on the FTC spyware workshop held in March of last year.[187] These included creating behavioural profiles of software in a standardized format that could be matched with user preferences. In this manner each piece of software could be graded based on its behaviours either by the software community or based on a standard set of criteria. Once a profile has been created in this manner the user's system can alert the user if the software does not match the user's preferences, and allow the user to decide whether to go through with the installation.

Additional standardization of the EULA and installation procedures generally is highly recommended. With standard EULA disclosures prevalent in the industry, it is foreseeable that software could be developed to 'read' a EULA for a user and report on any pre-selected behaviours that are important to the user. For example there could be one standard clause that addresses privacy concerns and has standard forms for different behaviours that the software may exhibit. If privacy is highlighted as a concern of the user, the software could read this clause and report in plain language the risk to the user, who could then investigate the clause if necessary. This kind of optional industry standardization may be a fantasy but if it were achieved it could go a long way towards granting users more knowledge of software functionality and control over its installation.

No doubt there are serious problems with relying solely on self-regulation to address all of spyware's problems due to the structure of the adware market.

[187] Staff Report, Federal Trade Commission. *Monitoring Software on Your PC: Spyware, Adware and Other Software* (Washington: Federal Trade Commission, 2005) at 16-17.

Nevertheless the industry could certainly help standardize installation procedures and make compliance easier when legislation is introduced.

Market solutions

Market solutions have gained prominence recently as large software companies join specialists in building increasingly powerful anti-spyware software for the public. According to surveys, spyware installations have dropped significantly since 2004. This trend can be attributed to several factors, including stronger anti-spyware solutions, better consumer awareness and the patching of severe security holes in Microsoft's Internet Explorer browser. This trend demonstrates that market solutions can have a significant impact, but spyware installations are still prevalent. While the successes of market driven solutions are to be commended, there are problems with relying on them too heavily.

The first is the lack of technical expertise among the general public. Those with knowledge of the industry would likely approach a reputable software company or conduct research before installing anti-spyware software. However a quick online search for 'anti-spyware software' will reveal thousands of results. Many alleged anti-spyware solutions are weak and would have little effect fighting spyware on a user's computer, while others are actually spyware themselves. Because of the difficulty many users face in finding software online, a purely market driven solution is not likely to be effective alone. Consumer education seems to be working to some extent in driving users towards legitimate free anti-spyware tools such as Microsoft anti-spyware, Spybot S&D and Lavasoft Ad-Aware, but these products are often not sufficient for the worst spyware infections.

Anti-spyware tools are also inherently imperfect and can never catch and remove every threat. Tests have shown that even the best performing anti-spyware programs will miss a quarter of critical files and registry entries.[188] The process of detecting and adding a piece of spyware to an anti-spyware database takes time. Researchers must first find the the malicious software on the Internet, then must test the software to find its signature (the pattern of files and registry changes that are made by the software on a user's computer.) This process can take weeks in itself, and the piece of spyware in question could have existed "in the wild" long before the anti-spyware researchers discovered it. A new Microsoft technology called 'Strider' aims to take a new approach by giving the user more control over software that starts itself automatically, but this project is still in the development stage.[189]

---

[188] Eric Howes "The Spyware Warrior Guide to Anti-Spyware Testing" *spywarewarrior.com* (October 2004), online: <http://spywarewarrior.com/asw-test-guide.htm>.
[189] Microsoft, *Strider Gatekeeper Spyware Management: Beyond Signature-based Approach* , online: <http://research.microsoft.com/spyware/>.

Anti-spyware software also provides no deterrence to spyware companies. If caught by an anti-spyware program, the spyware is at worst removed. Spyware companies are obviously never asked to compensate users for lost time and money by anti-spyware software. Hence while anti-spyware software is certainly an appreciated ally and its successes in recent months are commended, when addressing the spyware problem it is not a solution in and of itself. This is especially so given the ongoing litigation by spyware vendors against anti-spyware companies, which could potentially cripple anti-spyware commercial software distribution.

A quick cookie fix

Market solutions can certainly help to improve user control over tracking cookies. More useful security settings could be made available on browsers to provide users with meaningful protection against third-party cookies and better information about their privacy-invasive potential.

CONCLUSION

The movement to regulate software installations should not necessarily be viewed solely as a battle against spyware, even though this may have been its original goal. It should be aimed at the greater goals of clarifying uncertain law surrounding the legitimacy of clickwrap agreements and empowering users to better control their computers. Reining in spyware will be a natural and beneficial consequence of this action. Ira Rubenstein, counsel for Microsoft, recently demonstrated potential industry concerns while speaking at a US congressional committee investigating spyware: "Congress must proceed cautiously to ensure that such legislation targets the deceptive behavior of spyware publishers -- and not features or functionalities that have legitimate uses."[190] Focusing on the installation process instead of outlawing particular software functions should help to accommodate these concerns while establishing a strong reaction to the spyware problem.

[190] *Rubenstein*, *supra* note 163.

RECOMMENDATIONS

This report has identified a number of issues with spyware and suggested courses of actions to clarify the spyware issue for consumers, reduce its ill-effects and produce a fairer model for software installations. The following are the recommendations that are most likely to result in a substantial improvement in the spyware situation for consumers:

- Give a clear mandate and allocate resources towards the department best able to handle spyware complaints and enforce current laws against spyware activity.
- Enforce current consumer protection and competition laws against companies who engage in the worst spyware activity.
- Continue and strengthen consumer education initiatives regarding spyware, accentuating:
    - Only download from websites you trust;
    - Update your operating system software;
    - Install a trusted anti-spyware solution.
- Build support in the software community for clearer rules of installation for potentially unwanted software.
- Develop initiatives towards more accountability in the advertising industry, clarifying how advertising money gets to spyware distributors and what advertisers, advertising companies and brokers can do about it.
- Introduce spyware-specific legislation that:
    - Creates liability for software producers for the actions of their affiliates;
    - Clarifies the rules of installing potentially unwanted software by creating clear disclosure requirements;
    - Creates a higher threshold of consent for software installations than simple contractual consent, namely “fair and obvious” consent;
    - Creates a private right of action, with statutory damages, for unwanted installations of spyware;
    - Specifically empowers an agency with spyware enforcement and permits that agency to cooperate with foreign counterparts
    - Regulates the practice of targeting software installations towards children;
    - Requires standard uninstall procedures for all software;
    - Contains exemptions for operating systems.

APPENDIX I

The Pure Software Act: A Proposal for Mandatory Software Labeling

Simson L. Garfinkel
MIT Computer Science and Artificial Intelligence Laboratory
(Reproduced with the consent of Mr. Garfinkel)

Abstract

Spyware and adware are a scourge of desktop computing. Many of these programs appear to perform useful functions but have hidden purposes and code that are rarely in the user's interest. For example, Gator's eWallet program fills out web forms but also displays pop-up advertisements on a regular basis.[1] Some spyware programs go further by hiding the fact that they are running or by failing to provide "uninstall" scripts.

Adware and spyware is developed and sold by legitimate companies. These activities do not violate the Computer Fraud and Abuse Act (18 U.S.C. 1030)[2] because users consent to be monitored when they agree to overly-broad and turgid click-through license agreements.

The problem that computer users face today with spyware is remarkably similar to the problem that they faced a century ago with patent medicines. Just as programs today have undocumented functions, patent medicines had undocumented ingredients such as cocaine and codeine. Many people became addicted to such potions without even realizing it.

The solution to patent medicines was the 1906 Pure Food and Drug Act[3] --- legislation that forced companies selling a food and drugs in the United States to disclose certain ingredients on product labels. With the knowledge of what they were about to ingest, consumers were able to identify and avoid (if they wished) consuming potions that were "habit forming." Equipped with the information from thousands of labels, lawmakers were empowered to pass additional legislation in the public interest.

A similar approach can be applied to software. Federal regulations could require mandatory disclosure accompanying any program sold or distributed in the US. The label could consist of icons that documented specific program behaviors. These icons would be displayed at the top of license agreements, on install screens, and in key places such as the Windows "Add or Remove Programs" control panel. Some sample icons are shown in Figure 1.

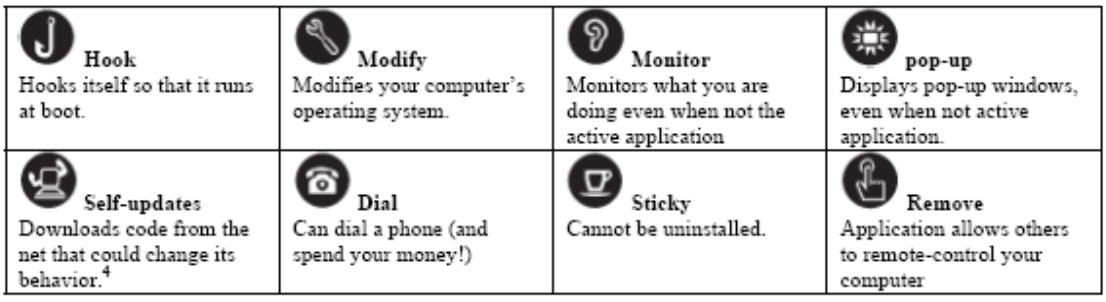


Figure 1: A few icons that could be required by federal regulation.

Icons are not necessarily bad. For example, the Google's Toolbar [sic], which is generally not regarded as a piece of spyware, would get the Hook, Modify, and Self-updates icons. With time, in fact, consumers might want to avoid programs that do not display the Self-updates icon, because these programs would not automatically patch themselves when new security flaws are discovered. The point of the icons is not to scare off all consumers, but to make visible functionality that is invisible today. Disclosure also helps academics, activists and lawmakers.

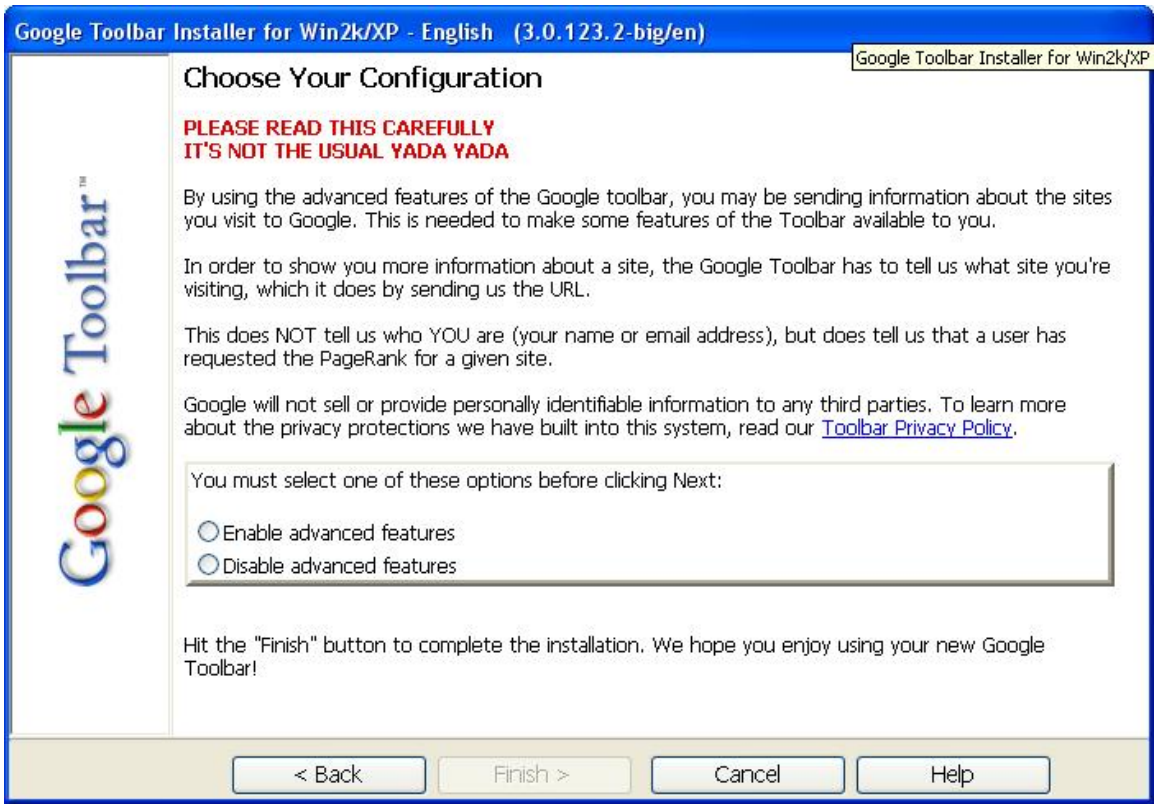
This 10-minute talk will discuss the history of the 1906 Act, show how similar justification can be used for software today, and make an initial proposal for icons and behaviors that would require disclosure.

[1] Barrett, Robertson, "Five Major Categories of Spyware," Special to Consumer WebWatch, October 21, 2002. http://www.consumerwebwatch.org/news/articles/spyware_categories.htm
[2] http://www.usdoj.gov/criminal/cybercrime/1030_new.html
[3] FDA Consumer, "The Story of the Laws Behind The Labels," Food and Drug Administration, June 1981. http://vm.cfsan.fda.gov/~lrd/history1.html
[4] Any update that added a new icon would presumably require explicit user consent.

APPENDIX II

Google's Internet Explorer Toolbar Installation

The Google toolbar's installation procedure has been widely regarded as an effective disclosure of potential unwanted software behaviour. As well as discussing the issue separately, on a screen dedicated solely to the topic and away from less important information, Google uses coloured text to bring the issue to the user's attention, makes the feature that exhibits the behaviour optional, and uses brief, plain language. Another strong feature of the disclosure is that it forces the user to perform an action beyond simply clicking 'finish' – the user must select a radio box before the 'finish' button becomes active, and **there is no default selection**. All these features combine to force the user to pay closer attention to the disclosure.



APPENDIX III

PIAC Survey results

QS1A CONCERNED WITH ID THEFT

How concerned are you with the following on the internet today...ID theft

	Total Respondents	Most Concerned (10,9)	Somewhat Concerned (8,7)	Neutral (6,5)	Somewhat Not Concerned (4,3)	Least Concerned (2,1)	Mean
TOTAL	(2152)	43%	27%	15%	9%	6%	7.5
QD1 AGE GROUP							
18-24	(132)	17%	29%	24%	17%	13%	5.9
25-34	(369)	39%	26%	16%	11%	8%	7.1
35-44	(566)	46%	26%	14%	9%	5%	7.6
45-54	(593)	44%	27%	15%	7%	6%	7.6
55-64	(345)	51%	26%	13%	7%	3%	8.0
65+	(136)	40%	31%	11%	10%	8%	7.4
Refused	(11)	56%	34%	11%	0%	0%	8.8
QD2 REGION CMA CA							
Newfoundland	(47)	45%	19%	15%	8%	14%	7.2
Nova Scotia	(192)	41%	27%	19%	7%	6%	7.4
New Brunswick	(135)	48%	22%	13%	11%	6%	7.5
Prince Edward Island	(18)	45%	18%	29%	0%	8%	7.5
Quebec	(169)	48%	24%	12%	8%	8%	7.6
Ontario	(516)	42%	27%	16%	9%	6%	7.5
Manitoba	(142)	43%	25%	19%	11%	3%	7.5
Saskatchewan	(74)	28%	29%	14%	20%	9%	6.5
Alberta	(437)	43%	30%	14%	9%	3%	7.6
British Columbia	(422)	38%	31%	15%	10%	5%	7.3
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	36%	21%	17%	11%	14%	6.7
$25,000 To Less Than $50,000	(492)	49%	25%	14%	8%	3%	7.8
$50,000 To Less Than $75,000	(488)	39%	31%	15%	8%	8%	7.3
$75,000 And Over	(659)	38%	29%	15%	12%	6%	7.3
Don't Know/Refused	(321)	53%	23%	13%	9%	3%	8.0
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	39%	34%	12%	8%	7%	7.4
2	(749)	44%	25%	15%	11%	5%	7.5
3	(424)	44%	24%	17%	8%	7%	7.4
4	(433)	43%	27%	16%	8%	7%	7.4
5	(159)	50%	26%	11%	9%	4%	7.8
6	(83)	33%	28%	20%	11%	8%	7.0
Refused	(3)	37%	17%	0%	46%	0%	6.7
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	44%	25%	15%	10%	6%	7.5
One	(262)	43%	23%	20%	10%	5%	7.4
Two	(189)	42%	28%	11%	9%	10%	7.3
Three	(40)	41%	19%	27%	9%	3%	7.3
Four Or More	(11)	48%	40%	8%	4%	0%	8.2
Refused	(218)	46%	24%	14%	9%	7%	7.5
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	44%	25%	15%	10%	6%	7.5
One	(275)	46%	23%	17%	10%	4%	7.5
Two	(151)	42%	26%	21%	7%	3%	7.6
Three	(34)	35%	35%	4%	10%	15%	7.0
Four Or More	(6)	43%	28%	20%	10%	0%	8.0
Refused	(218)	46%	24%	14%	9%	7%	7.5
QD6 EDUCATION							
Elementary School	(26)	88%	6%	3%	2%	1%	9.4
High School	(497)	47%	25%	15%	6%	7%	7.7
Community College	(615)	48%	23%	13%	10%	6%	7.6
University	(685)	37%	30%	16%	11%	6%	7.2
Post-Graduate/Professionot Availablel	(324)	38%	30%	16%	11%	5%	7.3
Don't Know/Refused	(5)	27%	0%	45%	27%	0%	6.0
QD8 GENDER							
Male	(1029)	37%	29%	15%	10%	9%	7.1
Female	(1123)	48%	25%	15%	9%	4%	7.8
QD9 GENDERATION							
Male - 18 To 34	(223)	30%	25%	15%	17%	12%	6.4
Male - 35 To 54	(529)	39%	33%	13%	9%	7%	7.4
Male - 55+	(277)	42%	29%	17%	5%	8%	7.5
Female - 18 To 34	(280)	36%	28%	21%	8%	6%	7.2
Female - 35 To 54	(637)	52%	21%	16%	8%	4%	7.9
Female - 55+	(206)	53%	25%	10%	10%	2%	8.1
QD11 REGION							
Atlantic	(393)	43%	25%	16%	8%	7%	7.4
Quebec	(168)	48%	24%	12%	8%	8%	7.6
Ontario	(515)	43%	27%	16%	9%	6%	7.5
Prairies	(652)	39%	29%	15%	12%	4%	7.4
British Columbia	(424)	39%	30%	15%	10%	5%	7.4
QD12 LANGUAGE							
English	(1999)	41%	28%	16%	9%	6%	7.4
French	(153)	50%	23%	11%	10%	6%	7.7

QS1B CONCERNED WITH SPYWARE

How concerned are you with the following on the internet today...Spyware ?

	Total Respondents	Most Concerned (10,9)	Somewhat Concerned (8,7)	Neutral (6,5)	Somewhat Not Concerned (4,3)	Least Concerned (2,1)	Mean
TOTAL	(2152)	43%	27%	16%	8%	6%	7.5
QD1 AGE GROUP							
18-24	(132)	30%	31%	22%	10%	7%	6.9
25-34	(369)	36%	32%	17%	9%	6%	7.2
35-44	(566)	44%	30%	14%	8%	4%	7.7
45-54	(593)	44%	26%	14%	10%	6%	7.5
55-64	(345)	50%	21%	18%	6%	5%	7.7
65+	(136)	44%	27%	14%	7%	8%	7.3
Refused	(11)	74%	15%	0%	11%	0%	8.7
QD2 REGION CMA CA							
Newfoundland	(47)	44%	24%	13%	8%	11%	7.3
Nova Scotia	(192)	46%	23%	18%	8%	5%	7.5
New Brunswick	(135)	41%	33%	16%	6%	5%	7.5
Prince Edward Island	(18)	53%	20%	14%	8%	6%	7.6
Quebec	(169)	47%	20%	18%	8%	7%	7.5
Ontario	(516)	42%	29%	15%	9%	5%	7.5
Manitoba	(142)	43%	27%	18%	9%	4%	7.5
Saskatchewan	(74)	32%	30%	14%	16%	8%	6.8
Alberta	(437)	40%	35%	15%	7%	3%	7.6
British Columbia	(422)	41%	30%	18%	7%	5%	7.5
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	37%	25%	18%	9%	11%	7.0
$25,000 To Less Than $50,000	(492)	45%	25%	18%	8%	4%	7.6
$50,000 To Less Than $75,000	(488)	39%	29%	18%	7%	7%	7.3
$75,000 And Over	(659)	39%	30%	14%	10%	7%	7.3
Don't Know/Refused	(321)	57%	22%	13%	6%	2%	8.2
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	39%	29%	18%	8%	6%	7.3
2	(749)	42%	26%	17%	9%	6%	7.4
3	(424)	45%	27%	15%	7%	6%	7.6
4	(433)	45%	26%	15%	9%	6%	7.5
5	(159)	50%	30%	9%	10%	2%	7.9
6	(83)	35%	26%	22%	7%	11%	6.9
Refused	(3)	37%	46%	17%	0%	0%	8.2
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	44%	26%	16%	8%	6%	7.5
One	(262)	45%	27%	17%	7%	4%	7.6
Two	(189)	43%	31%	9%	10%	7%	7.5
Three	(40)	50%	20%	17%	8%	5%	7.7
Four Or More	(11)	38%	33%	15%	0%	14%	7.2
Refused	(218)	46%	28%	13%	8%	5%	7.7
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	43%	27%	15%	9%	6%	7.4
One	(275)	46%	27%	16%	7%	4%	7.7
Two	(151)	45%	31%	16%	5%	3%	7.8
Three	(34)	36%	24%	15%	16%	10%	7.0
Four Or More	(6)	71%	0%	29%	0%	0%	8.5
Refused	(218)	46%	28%	13%	8%	5%	7.7
QD6 EDUCATION							
Elementary School	(26)	71%	6%	20%	1%	1%	8.7
High School	(497)	49%	24%	15%	6%	6%	7.7
Community College	(615)	43%	28%	17%	6%	5%	7.6
University	(685)	39%	29%	17%	11%	5%	7.3
Post-Graduate/Professionot Availablel	(324)	40%	27%	14%	11%	8%	7.2
Don't Know/Refused	(5)	27%	37%	14%	0%	22%	6.5
QD8 GENDER							
Male	(1029)	38%	30%	16%	10%	6%	7.2
Female	(1123)	48%	25%	16%	6%	5%	7.7
QD9 GENDERATION							
Male - 18 To 34	(223)	32%	32%	17%	11%	8%	7.0
Male - 35 To 54	(529)	38%	30%	14%	13%	4%	7.3
Male - 55+	(277)	42%	27%	17%	6%	8%	7.3
Female - 18 To 34	(280)	37%	31%	20%	7%	5%	7.3
Female - 35 To 54	(637)	50%	26%	14%	5%	5%	7.9
Female - 55+	(206)	53%	19%	17%	6%	4%	7.8
QD11 REGION							
Atlantic	(393)	44%	28%	15%	7%	6%	7.5
Quebec	(168)	48%	19%	18%	8%	8%	7.5
Ontario	(515)	42%	29%	15%	9%	5%	7.5
Prairies	(652)	39%	33%	15%	9%	4%	7.4
British Columbia	(424)	40%	31%	18%	7%	5%	7.5
QD12 LANGUAGE							
English	(1999)	42%	29%	16%	8%	5%	7.5
French	(153)	46%	21%	17%	8%	7%	7.5

QS1C CONCERNED WITH VIRUSES

How concerned are you with the following on the internet today...Viruses ?

	Total Respondents	Most Concerned (10,9)	Somewhat Concerned (8,7)	Neutral (6,5)	Somewhat Not Concerned (4,3)	Least Concerned (2,1)	Mean
TOTAL	(2152)	53%	24%	11%	7%	5%	7.9
QD1 AGE GROUP							
18-24	(132)	37%	34%	16%	10%	4%	7.3
25-34	(369)	42%	29%	15%	9%	6%	7.4
35-44	(566)	54%	27%	10%	5%	3%	8.1
45-54	(593)	59%	19%	11%	6%	5%	8.1
55-64	(345)	61%	19%	10%	4%	6%	8.2
65+	(136)	54%	24%	8%	11%	4%	7.9
Refused	(11)	57%	27%	4%	11%	0%	8.3
QD2 REGION CMA CA							
Newfoundland	(47)	57%	19%	8%	5%	11%	7.7
Nova Scotia	(192)	59%	23%	7%	7%	4%	8.2
New Brunswick	(135)	56%	24%	14%	4%	3%	8.1
Prince Edward Island	(18)	47%	2%	37%	8%	6%	7.2
Quebec	(169)	53%	22%	11%	7%	8%	7.8
Ontario	(516)	52%	25%	12%	8%	4%	7.9
Manitoba	(142)	57%	18%	12%	8%	6%	8.0
Saskatchewan	(74)	46%	32%	13%	3%	6%	7.7
Alberta	(437)	54%	26%	11%	6%	3%	8.1
British Columbia	(422)	52%	29%	10%	5%	4%	8.0
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	45%	27%	14%	7%	8%	7.5
$25,000 To Less Than $50,000	(492)	55%	25%	10%	6%	5%	8.0
$50,000 To Less Than $75,000	(488)	53%	24%	11%	8%	4%	8.0
$75,000 And Over	(659)	49%	25%	14%	7%	6%	7.7
Don't Know/Refused	(321)	64%	21%	8%	5%	3%	8.4
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	45%	30%	9%	10%	7%	7.5
2	(749)	53%	21%	14%	6%	6%	7.8
3	(424)	58%	23%	12%	5%	2%	8.3
4	(433)	55%	23%	10%	8%	4%	8.0
5	(159)	59%	28%	5%	4%	4%	8.4
6	(83)	52%	33%	6%	2%	7%	8.2
Refused	(3)	0%	63%	37%	0%	0%	7.1
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	55%	22%	12%	6%	4%	8.0
One	(262)	57%	23%	13%	3%	3%	8.2
Two	(189)	47%	25%	13%	7%	8%	7.6
Three	(40)	54%	33%	1%	1%	10%	8.0
Four Or More	(11)	31%	46%	23%	0%	0%	7.8
Refused	(218)	46%	31%	9%	10%	3%	7.8
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	53%	23%	13%	6%	5%	7.9
One	(275)	58%	23%	11%	4%	4%	8.2
Two	(151)	61%	29%	4%	6%	0%	8.6
Three	(34)	65%	21%	4%	0%	10%	8.3
Four Or More	(6)	90%	10%	0%	0%	0%	9.3
Refused	(218)	46%	31%	9%	10%	3%	7.8
QD6 EDUCATION							
Elementary School	(26)	71%	23%	5%	0%	1%	8.9
High School	(497)	60%	19%	8%	6%	6%	8.1
Community College	(615)	51%	27%	12%	6%	4%	8.0
University	(685)	50%	25%	11%	9%	5%	7.7
Post-Graduate/Professionot Availablel	(324)	50%	26%	14%	4%	6%	7.9
Don't Know/Refused	(5)	27%	37%	14%	0%	22%	6.8
QD8 GENDER							
Male	(1029)	46%	26%	13%	9%	5%	7.6
Female	(1123)	59%	22%	9%	4%	5%	8.2
QD9 GENDERATION							
Male - 18 To 34	(223)	33%	31%	16%	13%	7%	7.0
Male - 35 To 54	(529)	49%	26%	14%	6%	5%	7.8
Male - 55+	(277)	54%	22%	11%	10%	3%	7.9
Female - 18 To 34	(280)	48%	29%	14%	5%	4%	7.8
Female - 35 To 54	(637)	63%	21%	7%	5%	3%	8.4
Female - 55+	(206)	63%	19%	8%	3%	7%	8.3
QD11 REGION							
Atlantic	(393)	56%	21%	14%	5%	5%	8.0
Quebec	(168)	54%	21%	10%	7%	8%	7.8
Ontario	(515)	52%	24%	12%	8%	4%	7.9
Prairies	(652)	53%	26%	11%	6%	4%	8.0
British Columbia	(424)	52%	29%	10%	6%	3%	8.0
QD12 LANGUAGE							
English	(1999)	52%	25%	11%	7%	5%	7.9
French	(153)	55%	22%	12%	5%	6%	8.0

QS1D CONCERNED WITH SPAM

How concerned are you with the following on the internet today...Spam ?

	Total Respondents	Most Concerned (10,9)	Somewhat Concerned (8,7)	Neutral (6,5)	Somewhat Not Concerned (4,3)	Least Concerned (2,1)	Mean
TOTAL	(2152)	38%	26%	20%	9%	7%	7.1
QD1 AGE GROUP							
18-24	(132)	22%	19%	27%	17%	16%	5.8
25-34	(369)	26%	28%	24%	11%	11%	6.5
35-44	(566)	37%	26%	21%	11%	4%	7.2
45-54	(593)	44%	28%	17%	7%	4%	7.7
55-64	(345)	44%	24%	18%	7%	7%	7.5
65+	(136)	45%	25%	18%	8%	5%	7.5
Refused	(11)	62%	12%	15%	0%	11%	7.6
QD2 REGION CMA CA							
Newfoundland	(47)	32%	25%	16%	11%	16%	6.6
Nova Scotia	(192)	39%	20%	24%	11%	5%	7.0
New Brunswick	(135)	41%	28%	17%	9%	4%	7.4
Prince Edward Island	(18)	47%	10%	20%	16%	8%	7.0
Quebec	(169)	39%	27%	15%	6%	12%	7.2
Ontario	(516)	38%	25%	22%	10%	5%	7.2
Manitoba	(142)	36%	24%	23%	12%	5%	7.1
Saskatchewan	(74)	25%	20%	33%	10%	11%	6.3
Alberta	(437)	39%	24%	23%	11%	3%	7.3
British Columbia	(422)	34%	28%	21%	10%	5%	7.1
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	29%	30%	19%	8%	14%	6.7
$25,000 To Less Than $50,000	(492)	39%	26%	22%	8%	5%	7.3
$50,000 To Less Than $75,000	(488)	35%	25%	19%	12%	9%	6.9
$75,000 And Over	(659)	35%	26%	22%	10%	7%	7.0
Don't Know/Refused	(321)	50%	23%	17%	7%	3%	7.8
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	42%	23%	14%	10%	11%	7.1
2	(749)	39%	26%	20%	9%	7%	7.2
3	(424)	35%	27%	24%	11%	3%	7.2
4	(433)	39%	24%	23%	7%	6%	7.2
5	(159)	34%	34%	18%	7%	7%	7.3
6	(83)	24%	23%	28%	13%	13%	6.2
Refused	(3)	0%	37%	17%	46%	0%	5.7
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	38%	27%	21%	8%	6%	7.3
One	(262)	36%	27%	23%	11%	5%	7.1
Two	(189)	30%	20%	26%	15%	9%	6.5
Three	(40)	39%	28%	10%	3%	19%	7.0
Four Or More	(11)	8%	31%	44%	0%	17%	5.9
Refused	(218)	41%	23%	14%	13%	10%	7.0
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	36%	25%	22%	9%	7%	7.1
One	(275)	40%	27%	20%	9%	5%	7.3
Two	(151)	43%	31%	17%	8%	2%	7.8
Three	(34)	25%	33%	26%	6%	11%	6.8
Four Or More	(6)	20%	39%	41%	0%	0%	6.9
Refused	(218)	41%	23%	14%	13%	10%	7.0
QD6 EDUCATION							
Elementary School	(26)	42%	6%	37%	8%	6%	7.3
High School	(497)	43%	23%	19%	8%	7%	7.4
Community College	(615)	36%	28%	22%	9%	6%	7.2
University	(685)	36%	27%	19%	11%	8%	7.0
Post-Graduate/Professionot Availablel	(324)	37%	24%	23%	8%	8%	7.1
Don't Know/Refused	(5)	27%	10%	22%	41%	0%	6.2
QD8 GENDER							
Male	(1029)	33%	26%	22%	11%	8%	6.8
Female	(1123)	42%	25%	19%	8%	6%	7.4
QD9 GENDERATION							
Male - 18 To 34	(223)	23%	25%	20%	15%	17%	5.9
Male - 35 To 54	(529)	37%	27%	22%	10%	5%	7.2
Male - 55+	(277)	36%	26%	25%	7%	6%	7.1
Female - 18 To 34	(280)	27%	26%	30%	10%	8%	6.6
Female - 35 To 54	(637)	44%	28%	17%	8%	3%	7.7
Female - 55+	(206)	50%	22%	14%	7%	7%	7.7
QD11 REGION							
Atlantic	(393)	38%	22%	22%	10%	7%	7.1
Quebec	(168)	40%	27%	14%	7%	12%	7.2
Ontario	(515)	38%	25%	22%	10%	5%	7.2
Prairies	(652)	36%	24%	25%	11%	5%	7.1
British Columbia	(424)	34%	29%	21%	11%	5%	7.0
QD12 LANGUAGE							
English	(1999)	37%	25%	22%	10%	6%	7.1
French	(153)	41%	27%	15%	7%	11%	7.2

QS1E PROTECT CHILDREN FRM ADULT CONTENT

How concerned are you with the following on the internet today...Protecting children from adult content?

	Total Respondents	Most Concerned (10,9)	Somewhat Concerned (8,7)	Neutral (6,5)	Somewhat Not Concerned (4,3)	Least Concerned (2,1)	Mean
TOTAL	(2152)	46%	16%	15%	7%	16%	6.9
QD1 AGE GROUP							
18-24	(132)	17%	18%	25%	10%	30%	5.1
25-34	(369)	41%	15%	14%	9%	22%	6.4
35-44	(566)	52%	19%	13%	8%	8%	7.6
45-54	(593)	46%	18%	15%	7%	13%	7.1
55-64	(345)	54%	11%	15%	5%	16%	7.3
65+	(136)	42%	17%	12%	8%	21%	6.5
Refused	(11)	64%	0%	6%	15%	15%	7.3
QD2 REGION CMA CA							
Newfoundland	(47)	47%	19%	18%	1%	15%	7.3
Nova Scotia	(192)	50%	13%	10%	9%	18%	7.0
New Brunswick	(135)	58%	11%	17%	8%	7%	7.7
Prince Edward Island	(18)	35%	45%	0%	0%	20%	7.2
Quebec	(169)	41%	17%	21%	5%	15%	6.8
Ontario	(516)	48%	13%	13%	8%	18%	6.9
Manitoba	(142)	52%	12%	14%	8%	14%	7.2
Saskatchewan	(74)	41%	23%	9%	8%	19%	6.7
Alberta	(437)	46%	18%	13%	9%	14%	7.1
British Columbia	(422)	45%	18%	12%	7%	17%	6.9
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	39%	17%	10%	9%	24%	6.4
$25,000 To Less Than $50,000	(492)	52%	13%	15%	8%	13%	7.2
$50,000 To Less Than $75,000	(488)	47%	15%	14%	6%	17%	7.0
$75,000 And Over	(659)	38%	19%	17%	8%	18%	6.6
Don't Know/Refused	(321)	54%	12%	15%	7%	12%	7.4
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	41%	10%	18%	6%	25%	6.2
2	(749)	41%	17%	16%	7%	19%	6.6
3	(424)	49%	14%	14%	10%	14%	7.1
4	(433)	51%	20%	11%	7%	11%	7.5
5	(159)	55%	14%	15%	9%	7%	7.7
6	(83)	56%	19%	15%	5%	5%	7.9
Refused	(3)	37%	0%	63%	0%	0%	7.3
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	42%	17%	15%	8%	18%	6.7
One	(262)	62%	17%	11%	6%	5%	8.2
Two	(189)	60%	19%	10%	9%	2%	8.2
Three	(40)	78%	10%	3%	7%	2%	8.9
Four Or More	(11)	58%	16%	26%	0%	0%	8.3
Refused	(218)	39%	10%	20%	6%	24%	6.1
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	45%	17%	14%	7%	17%	6.9
One	(275)	52%	15%	17%	10%	6%	7.5
Two	(151)	57%	26%	6%	5%	5%	8.2
Three	(34)	51%	10%	14%	14%	11%	7.2
Four Or More	(6)	43%	10%	48%	0%	0%	7.3
Refused	(218)	39%	10%	20%	6%	24%	6.1
QD6 EDUCATION							
Elementary School	(26)	63%	21%	2%	2%	12%	8.1
High School	(497)	54%	14%	12%	9%	12%	7.4
Community College	(615)	50%	17%	14%	5%	14%	7.3
University	(685)	40%	14%	19%	8%	19%	6.4
Post-Graduate/Professionot Availablel	(324)	38%	20%	13%	8%	21%	6.5
Don't Know/Refused	(5)	0%	10%	41%	0%	49%	4.0
QD8 GENDER							
Male	(1029)	36%	17%	17%	10%	20%	6.3
Female	(1123)	55%	14%	13%	5%	13%	7.5
QD9 GENDERATION							
Male - 18 To 34	(223)	29%	13%	17%	11%	30%	5.4
Male - 35 To 54	(529)	41%	21%	17%	10%	11%	7.0
Male - 55+	(277)	35%	16%	17%	8%	25%	6.0
Female - 18 To 34	(280)	39%	19%	17%	7%	18%	6.7
Female - 35 To 54	(637)	57%	16%	12%	5%	11%	7.7
Female - 55+	(206)	64%	9%	13%	3%	11%	7.9
QD11 REGION							
Atlantic	(393)	50%	15%	16%	6%	13%	7.2
Quebec	(168)	41%	18%	21%	5%	15%	6.8
Ontario	(515)	48%	13%	13%	8%	18%	6.9
Prairies	(652)	46%	18%	13%	8%	15%	7.0
British Columbia	(424)	45%	18%	11%	8%	19%	6.8
QD12 LANGUAGE							
English	(1999)	47%	15%	13%	9%	17%	6.9
French	(153)	42%	18%	23%	3%	15%	6.9

QS1F CONCERNED WITH MODEM HIJACKING

How concerned are you with the following on the internet today...Modem hijacking ?

	Total Respondents	Most Concerned (10,9)	Somewhat Concerned (8,7)	Neutral (6,5)	Somewhat Not Concerned (4,3)	Least Concerned (2,1)	Mean
TOTAL	(2152)	38%	19%	18%	11%	14%	6.7
QD1 AGE GROUP							
18-24	(132)	16%	26%	19%	14%	25%	5.3
25-34	(369)	27%	23%	21%	12%	17%	6.1
35-44	(566)	41%	16%	17%	12%	13%	6.7
45-54	(593)	38%	19%	18%	11%	13%	6.8
55-64	(345)	50%	13%	18%	9%	9%	7.3
65+	(136)	40%	22%	10%	9%	19%	6.7
Refused	(11)	51%	18%	15%	15%	0%	7.7
QD2 REGION CMA CA							
Newfoundland	(47)	39%	15%	24%	10%	12%	6.7
Nova Scotia	(192)	47%	16%	16%	9%	12%	7.1
New Brunswick	(135)	42%	23%	16%	6%	13%	7.1
Prince Edward Island	(18)	39%	37%	0%	0%	24%	6.9
Quebec	(169)	42%	15%	17%	11%	15%	6.8
Ontario	(516)	36%	19%	18%	12%	15%	6.5
Manitoba	(142)	41%	12%	19%	17%	12%	6.7
Saskatchewan	(74)	28%	32%	19%	6%	14%	6.5
Alberta	(437)	39%	22%	18%	11%	10%	6.9
British Columbia	(422)	36%	20%	19%	10%	15%	6.6
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	32%	26%	17%	6%	19%	6.4
$25,000 To Less Than $50,000	(492)	47%	17%	18%	9%	10%	7.2
$50,000 To Less Than $75,000	(488)	37%	16%	18%	11%	18%	6.4
$75,000 And Over	(659)	29%	21%	18%	16%	17%	6.1
Don't Know/Refused	(321)	49%	17%	17%	9%	7%	7.4
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	36%	18%	22%	10%	14%	6.5
2	(749)	39%	19%	16%	11%	14%	6.7
3	(424)	40%	17%	19%	13%	11%	6.8
4	(433)	39%	17%	18%	11%	15%	6.7
5	(159)	41%	20%	9%	7%	22%	6.5
6	(83)	27%	27%	21%	14%	10%	6.5
Refused	(3)	0%	17%	83%	0%	0%	5.8
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	39%	18%	18%	11%	14%	6.7
One	(262)	44%	22%	15%	9%	10%	7.2
Two	(189)	36%	17%	13%	15%	20%	6.2
Three	(40)	35%	16%	18%	17%	15%	6.0
Four Or More	(11)	23%	42%	12%	13%	11%	6.6
Refused	(218)	37%	18%	17%	12%	15%	6.6
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	39%	18%	17%	11%	15%	6.6
One	(275)	37%	19%	18%	13%	12%	6.7
Two	(151)	44%	21%	18%	7%	10%	7.2
Three	(34)	37%	16%	17%	7%	24%	6.5
Four Or More	(6)	43%	28%	20%	10%	0%	7.7
Refused	(218)	37%	18%	17%	12%	15%	6.6
QD6 EDUCATION							
Elementary School	(26)	58%	25%	10%	3%	4%	8.3
High School	(497)	46%	19%	15%	8%	12%	7.2
Community College	(615)	46%	18%	13%	11%	11%	7.1
University	(685)	29%	18%	24%	12%	18%	6.1
Post-Graduate/Professionot Availablel	(324)	31%	19%	17%	16%	17%	6.2
Don't Know/Refused	(5)	0%	27%	73%	0%	0%	6.4
QD8 GENDER							
Male	(1029)	30%	20%	17%	13%	20%	6.1
Female	(1123)	45%	17%	19%	9%	9%	7.2
QD9 GENDERATION							
Male - 18 To 34	(223)	18%	24%	17%	12%	28%	5.3
Male - 35 To 54	(529)	33%	18%	19%	15%	16%	6.2
Male - 55+	(277)	39%	19%	14%	12%	17%	6.6
Female - 18 To 34	(280)	30%	24%	23%	13%	11%	6.4
Female - 35 To 54	(637)	47%	18%	17%	9%	9%	7.3
Female - 55+	(206)	55%	12%	18%	7%	8%	7.6
QD11 REGION							
Atlantic	(393)	41%	18%	19%	8%	13%	6.9
Quebec	(168)	43%	15%	16%	11%	15%	6.8
Ontario	(515)	36%	19%	18%	12%	16%	6.5
Prairies	(652)	37%	22%	19%	11%	11%	6.8
British Columbia	(424)	36%	19%	19%	11%	14%	6.6
QD12 LANGUAGE							
English	(1999)	37%	19%	18%	11%	15%	6.6
French	(153)	42%	16%	16%	13%	13%	6.8

QS2 SPYWARE POSES THREAT TO PRIVACY

Do you think spyware poses a threat to your personal privacy?

	Total Respondents	Yes	No
TOTAL	(2152)	91%	9%
QD1 AGE GROUP			
18-24	(132)	88%	12%
25-34	(369)	94%	6%
35-44	(566)	92%	8%
45-54	(593)	92%	8%
55-64	(345)	87%	13%
65+	(136)	87%	13%
Refused	(11)	97%	3%
QD2 REGION CMA CA			
Newfoundland	(47)	91%	9%
Nova Scotia	(192)	92%	8%
New Brunswick	(135)	91%	9%
Prince Edward Island	(18)	86%	14%
Quebec	(169)	89%	11%
Ontario	(516)	91%	9%
Manitoba	(142)	90%	10%
Saskatchewan	(74)	88%	12%
Alberta	(437)	92%	8%
British Columbia	(422)	92%	8%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	90%	10%
$25,000 To Less Than $50,000	(492)	93%	7%
$50,000 To Less Than $75,000	(488)	90%	10%
$75,000 And Over	(659)	89%	11%
Don't Know/Refused	(321)	92%	8%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	84%	16%
2	(749)	91%	9%
3	(424)	93%	7%
4	(433)	93%	7%
5	(159)	93%	7%
6	(83)	93%	7%
Refused	(3)	100%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	92%	8%
One	(262)	93%	7%
Two	(189)	93%	7%
Three	(40)	95%	5%
Four Or More	(11)	100%	0%
Refused	(218)	89%	11%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	92%	8%
One	(275)	94%	6%
Two	(151)	93%	7%
Three	(34)	86%	14%
Four Or More	(6)	100%	0%
Refused	(218)	89%	11%
QD6 EDUCATION			
Elementary School	(26)	99%	1%
High School	(497)	89%	11%
Community College	(615)	92%	8%
University	(685)	91%	9%
Post-Graduate/Professionot Availablel	(324)	89%	11%
Don't Know/Refused	(5)	100%	0%
QD8 GENDER			
Male	(1029)	91%	9%
Female	(1123)	90%	10%
QD9 GENDERATION			
Male - 18 To 34	(223)	92%	8%
Male - 35 To 54	(529)	91%	9%
Male - 55+	(277)	89%	11%
Female - 18 To 34	(280)	93%	7%
Female - 35 To 54	(637)	93%	7%
Female - 55+	(206)	85%	15%
QD11 REGION			
Atlantic	(393)	92%	8%
Quebec	(168)	89%	11%
Ontario	(515)	91%	9%
Prairies	(652)	91%	9%
British Columbia	(424)	92%	8%
QD12 LANGUAGE			
English	(1999)	90%	10%
French	(153)	91%	9%

QS3 CONCERNS MOST ABOUT SPYWARE

From the following list which one concerns you most about spyware?

	Total Respondents	Privacy concerns	Popups	Computer slowdowns and malfunctions	Browser hijacking	Don't Know/Not Applicable
TOTAL	(1883)	60%	4%	25%	9%	2%
QD1 AGE GROUP						
18-24	(112)	35%	5%	43%	14%	2%
25-34	(337)	57%	4%	30%	8%	2%
35-44	(498)	59%	2%	26%	9%	3%
45-54	(528)	66%	3%	22%	8%	2%
55-64	(290)	69%	5%	15%	8%	2%
65+	(108)	56%	3%	28%	13%	1%
Refused	(10)	62%	0%	24%	15%	0%
QD2 REGION CMA CA						
Newfoundland	(38)	53%	4%	31%	4%	8%
Nova Scotia	(170)	59%	3%	30%	7%	1%
New Brunswick	(117)	64%	2%	21%	10%	2%
Prince Edward Island	(13)	79%	10%	0%	0%	10%
Quebec	(151)	72%	3%	19%	5%	1%
Ontario	(447)	56%	4%	25%	13%	2%
Manitoba	(120)	49%	7%	33%	9%	2%
Saskatchewan	(65)	61%	7%	23%	3%	5%
Alberta	(385)	60%	2%	28%	8%	2%
British Columbia	(377)	53%	4%	31%	9%	3%
QD3 HOUSEHOLD INCOME						
Less Than $25,000	(168)	54%	7%	30%	8%	1%
$25,000 To Less Than $50,000	(431)	60%	5%	24%	9%	3%
$50,000 To Less Than $75,000	(441)	61%	2%	28%	7%	1%
$75,000 And Over	(565)	59%	4%	24%	12%	2%
Don't Know/Refused	(278)	67%	2%	18%	9%	3%
QD3A PEOPLE IN HOUSEHOLD						
1	(264)	54%	7%	31%	8%	1%
2	(656)	63%	3%	22%	9%	3%
3	(370)	62%	3%	26%	6%	2%
4	(380)	60%	3%	22%	12%	3%
5	(140)	53%	3%	27%	15%	2%
6	(70)	65%	6%	25%	4%	0%
Refused	(3)	100%	0%	0%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE						
None	(1190)	60%	3%	24%	10%	2%
One	(228)	67%	3%	18%	10%	3%
Two	(163)	66%	4%	22%	6%	2%
Three	(36)	63%	3%	27%	7%	0%
Four Or More	(10)	59%	0%	41%	0%	0%
Refused	(194)	60%	7%	26%	6%	1%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE						
None	(1218)	63%	3%	23%	9%	2%
One	(244)	55%	4%	28%	11%	2%
Two	(129)	52%	6%	23%	15%	5%
Three	(32)	78%	3%	20%	0%	0%
Four Or More	(4)	32%	0%	68%	0%	0%
Refused	(194)	60%	7%	26%	6%	1%
QD6 EDUCATION						
Elementary School	(24)	74%	0%	4%	22%	0%
High School	(429)	65%	3%	23%	9%	1%
Community College	(539)	59%	2%	26%	9%	3%
University	(596)	57%	5%	28%	8%	1%
Post-Graduate/Professionot Availablel	(290)	63%	4%	20%	10%	2%
Don't Know/Refused	(5)	63%	0%	37%	0%	0%
QD8 GENDER						
Male	(900)	57%	3%	28%	10%	1%
Female	(983)	63%	4%	22%	8%	3%
QD9 GENDERATION						
Male - 18 To 34	(200)	46%	5%	40%	9%	0%
Male - 35 To 54	(472)	61%	1%	26%	10%	1%
Male - 55+	(228)	63%	5%	20%	12%	1%
Female - 18 To 34	(251)	56%	3%	27%	10%	3%
Female - 35 To 54	(560)	64%	3%	22%	7%	4%
Female - 55+	(172)	68%	5%	16%	8%	3%
QD11 REGION						
Atlantic	(339)	61%	3%	26%	7%	3%
Quebec	(150)	72%	3%	19%	5%	1%
Ontario	(447)	56%	4%	25%	13%	2%
Prairies	(569)	58%	4%	28%	8%	2%
British Columbia	(378)	54%	4%	31%	9%	3%
QD12 LANGUAGE						
English	(1745)	57%	4%	26%	10%	2%
French	(138)	71%	3%	20%	4%	2%

QS41 spyware response

What have you done in response to spyware?

	Total Respondents	QS4 HAVE DONE IN RESPONSE TO SPYWARE					
		Reduced your time online	Stopped going online	Reduced your shopping online	Stopped shopping online	Reduced viewing certain websites	Stopped viewing certain websites
TOTAL	(1970)	9%	0%	8%	10%	16%	18%
QD1 AGE GROUP							
18-24	(118)	5%	1%	7%	15%	24%	14%
25-34	(347)	10%	1%	7%	9%	20%	17%
35-44	(524)	8%	0%	8%	8%	16%	18%
45-54	(547)	8%	1%	10%	10%	14%	17%
55-64	(307)	10%	0%	8%	11%	12%	22%
65+	(117)	10%	0%	6%	10%	12%	21%
Refused	(10)	19%	0%	14%	28%	25%	13%
QD2 REGION CMA CA							
Newfoundland	(42)	9%	0%	6%	8%	16%	10%
Nova Scotia	(177)	10%	0%	10%	8%	17%	19%
New Brunswick	(124)	12%	2%	12%	10%	18%	16%
Prince Edward Island	(15)	0%	0%	0%	16%	11%	18%
Quebec	(156)	10%	1%	5%	14%	14%	16%
Ontario	(468)	8%	0%	8%	8%	16%	19%
Manitoba	(129)	9%	1%	8%	9%	17%	19%
Saskatchewan	(67)	5%	0%	9%	8%	20%	24%
Alberta	(402)	10%	0%	10%	13%	19%	21%
British Columbia	(390)	8%	0%	9%	6%	13%	21%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(174)	8%	3%	4%	18%	21%	18%
$25,000 To Less Than $50,000	(455)	8%	0%	9%	7%	12%	19%
$50,000 To Less Than $75,000	(452)	9%	0%	7%	10%	14%	15%
$75,000 And Over	(595)	6%	0%	8%	8%	16%	17%
Don't Know/Refused	(294)	17%	1%	10%	15%	19%	26%
QD3A PEOPLE IN HOUSEHOLD							
1	(273)	8%	0%	6%	6%	16%	16%
2	(679)	11%	0%	8%	12%	13%	19%
3	(388)	9%	2%	10%	9%	14%	16%
4	(401)	8%	1%	8%	11%	20%	20%
5	(147)	8%	0%	10%	8%	22%	22%
6	(79)	5%	0%	4%	12%	14%	19%
Refused	(3)	0%	0%	0%	0%	46%	46%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1240)	10%	0%	8%	11%	14%	18%
One	(241)	9%	2%	14%	8%	18%	19%
Two	(175)	6%	1%	5%	10%	27%	24%
Three	(38)	11%	0%	1%	21%	14%	34%
Four Or More	(11)	0%	0%	11%	8%	27%	20%
Refused	(200)	10%	0%	5%	6%	18%	16%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1268)	9%	1%	8%	11%	14%	18%
One	(257)	8%	1%	8%	9%	20%	17%
Two	(142)	9%	0%	12%	11%	23%	25%
Three	(32)	10%	0%	13%	12%	38%	20%
Four Or More	(6)	0%	0%	0%	10%	10%	23%
Refused	(200)	10%	0%	5%	6%	18%	16%
QD6 EDUCATION							
Elementary School	(25)	6%	0%	13%	9%	20%	8%
High School	(449)	12%	1%	6%	13%	16%	23%
Community College	(569)	8%	1%	7%	10%	15%	17%
University	(626)	8%	0%	9%	8%	16%	19%
Post-Graduate/Professionot Availablel	(296)	8%	0%	10%	11%	14%	15%
Don't Know/Refused	(5)	0%	0%	0%	0%	41%	41%
QD8 GENDER							
Male	(934)	9%	0%	7%	10%	18%	19%
Female	(1036)	9%	1%	8%	10%	14%	18%
QD9 GENDERATION							
Male - 18 To 34	(208)	10%	1%	6%	11%	23%	18%
Male - 35 To 54	(484)	6%	0%	7%	8%	18%	17%
Male - 55+	(242)	12%	0%	8%	10%	14%	24%
Female - 18 To 34	(259)	9%	1%	8%	9%	20%	14%
Female - 35 To 54	(593)	9%	1%	10%	10%	12%	18%
Female - 55+	(184)	9%	0%	7%	12%	11%	20%
QD11 REGION							
Atlantic	(359)	10%	1%	9%	9%	17%	17%
Quebec	(155)	10%	1%	5%	14%	14%	16%
Ontario	(467)	8%	0%	8%	8%	16%	19%
Prairies	(598)	9%	0%	10%	11%	18%	22%
British Columbia	(391)	8%	0%	9%	6%	14%	20%
QD12 LANGUAGE							
English	(1827)	9%	0%	8%	9%	16%	19%
French	(143)	10%	1%	6%	15%	14%	16%

{sh (Continued)}

QS41 spyware response

What have you done in response to spyware?

	QS4 HAVE DONE IN RESPONSE TO SPYWARE					
	Reduced using e-mail	Stopped using e-mail	Installed anti-spyware software	Installed a firewall or router	Bought a new computer	Done nothing
TOTAL	4%	0%	71%	56%	5%	10%
QD1 AGE GROUP						
18-24	3%	0%	69%	53%	4%	14%
25-34	6%	1%	73%	57%	5%	12%
35-44	4%	0%	70%	59%	5%	8%
45-54	3%	0%	72%	60%	4%	8%
55-64	3%	0%	70%	52%	6%	13%
65+	3%	0%	71%	54%	10%	8%
Refused	13%	0%	72%	75%	11%	0%
QD2 REGION CMA CA						
Newfoundland	0%	0%	69%	66%	6%	12%
Nova Scotia	2%	0%	73%	60%	2%	9%
New Brunswick	3%	0%	69%	41%	8%	12%
Prince Edward Island	16%	0%	70%	36%	0%	18%
Quebec	2%	0%	60%	49%	3%	15%
Ontario	4%	1%	76%	56%	6%	9%
Manitoba	7%	0%	72%	49%	3%	9%
Saskatchewan	7%	0%	75%	57%	9%	12%
Alberta	8%	0%	76%	67%	8%	8%
British Columbia	2%	0%	73%	67%	7%	8%
QD3 HOUSEHOLD INCOME						
Less Than $25,000	3%	1%	68%	46%	3%	13%
$25,000 To Less Than $50,000	4%	0%	68%	56%	5%	12%
$50,000 To Less Than $75,000	6%	0%	70%	57%	5%	13%
$75,000 And Over	3%	0%	75%	57%	7%	9%
Don't Know/Refused	3%	0%	73%	62%	6%	6%
QD3A PEOPLE IN HOUSEHOLD						
1	4%	0%	70%	50%	3%	15%
2	3%	0%	70%	58%	7%	12%
3	3%	0%	72%	54%	5%	9%
4	6%	0%	73%	59%	5%	7%
5	3%	0%	71%	59%	3%	5%
6	8%	0%	76%	65%	5%	11%
Refused	0%	0%	63%	63%	0%	37%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE						
None	4%	0%	71%	58%	6%	10%
One	3%	0%	68%	56%	5%	11%
Two	5%	0%	79%	56%	5%	8%
Three	19%	0%	88%	36%	2%	7%
Four Or More	4%	0%	65%	79%	0%	26%
Refused	3%	0%	72%	51%	3%	16%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE						
None	4%	0%	72%	56%	6%	11%
One	5%	1%	71%	62%	4%	8%
Two	3%	1%	63%	61%	6%	4%
Three	11%	0%	74%	56%	0%	0%
Four Or More	0%	0%	90%	87%	20%	0%
Refused	3%	0%	72%	51%	3%	16%
QD6 EDUCATION						
Elementary School	2%	0%	71%	61%	6%	6%
High School	4%	0%	72%	61%	4%	8%
Community College	5%	0%	76%	55%	6%	8%
University	4%	1%	70%	54%	5%	13%
Post-Graduate/Professionot Availablel	2%	0%	63%	56%	6%	12%
Don't Know/Refused	0%	0%	86%	37%	0%	0%
QD8 GENDER						
Male	4%	0%	77%	61%	6%	8%
Female	4%	0%	65%	52%	5%	13%
QD9 GENDERATION						
Male - 18 To 34	5%	1%	80%	65%	5%	5%
Male - 35 To 54	4%	0%	77%	63%	5%	8%
Male - 55+	4%	0%	77%	56%	9%	9%
Female - 18 To 34	5%	1%	65%	47%	4%	20%
Female - 35 To 54	4%	0%	66%	56%	4%	8%
Female - 55+	2%	0%	65%	50%	6%	14%
QD11 REGION						
Atlantic	2%	0%	72%	52%	5%	10%
Quebec	2%	0%	60%	50%	3%	16%
Ontario	4%	1%	76%	56%	6%	9%
Prairies	7%	0%	75%	61%	7%	9%
British Columbia	2%	0%	74%	67%	7%	7%
QD12 LANGUAGE						
English	4%	0%	75%	58%	6%	9%
French	2%	0%	56%	51%	2%	17%

QS5 HAD SPYWARE ON HOME COMPUTER

Have you ever had spyware on your home computer(s)?

	Total Respondents	Yes	Not applicable (no home computer)	Don't know	No
TOTAL	(2152)	57%	21%	1%	21%
QD1 AGE GROUP					
18-24	(132)	68%	14%	2%	17%
25-34	(369)	63%	18%	1%	19%
35-44	(566)	64%	14%	3%	19%
45-54	(593)	58%	22%	1%	19%
55-64	(345)	44%	32%	0%	24%
65+	(136)	51%	18%	0%	31%
Refused	(11)	25%	35%	0%	40%
QD2 REGION CMA CA					
Newfoundland	(47)	54%	11%	4%	31%
Nova Scotia	(192)	63%	12%	1%	23%
New Brunswick	(135)	54%	19%	1%	27%
Prince Edward Island	(18)	73%	2%	0%	25%
Quebec	(169)	40%	38%	1%	21%
Ontario	(516)	64%	15%	1%	20%
Manitoba	(142)	64%	16%	3%	18%
Saskatchewan	(74)	59%	15%	0%	25%
Alberta	(437)	63%	16%	1%	19%
British Columbia	(422)	63%	16%	1%	20%
QD3 HOUSEHOLD INCOME					
Less Than $25,000	(192)	56%	27%	0%	17%
$25,000 To Less Than $50,000	(492)	52%	18%	1%	29%
$50,000 To Less Than $75,000	(488)	56%	25%	1%	17%
$75,000 And Over	(659)	60%	20%	1%	19%
Don't Know/Refused	(321)	61%	17%	2%	21%
QD3A PEOPLE IN HOUSEHOLD					
1	(301)	57%	25%	2%	16%
2	(749)	53%	25%	1%	21%
3	(424)	57%	18%	2%	23%
4	(433)	61%	16%	0%	23%
5	(159)	66%	12%	1%	21%
6	(83)	54%	24%	0%	22%
Refused	(3)	63%	37%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE					
None	(1357)	56%	22%	1%	21%
One	(262)	62%	13%	2%	23%
Two	(189)	54%	18%	0%	27%
Three	(40)	66%	16%	0%	17%
Four Or More	(11)	47%	35%	0%	18%
Refused	(218)	63%	19%	2%	15%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE					
None	(1393)	55%	22%	1%	22%
One	(275)	67%	12%	1%	21%
Two	(151)	63%	18%	1%	18%
Three	(34)	39%	33%	0%	29%
Four Or More	(6)	51%	20%	0%	29%
Refused	(218)	63%	19%	2%	15%
QD6 EDUCATION					
Elementary School	(26)	68%	18%	3%	11%
High School	(497)	56%	26%	1%	18%
Community College	(615)	59%	17%	1%	23%
University	(685)	59%	18%	1%	21%
Post-Graduate/Professionot Availablel	(324)	50%	27%	1%	22%
Don't Know/Refused	(5)	86%	14%	0%	0%
QD8 GENDER					
Male	(1029)	68%	17%	1%	14%
Female	(1123)	47%	25%	1%	27%
QD9 GENDERATION					
Male - 18 To 34	(223)	76%	15%	0%	8%
Male - 35 To 54	(529)	68%	17%	1%	14%
Male - 55+	(277)	61%	19%	1%	20%
Female - 18 To 34	(280)	52%	18%	1%	28%
Female - 35 To 54	(637)	54%	19%	2%	25%
Female - 55+	(206)	35%	36%	0%	29%
QD11 REGION					
Atlantic	(393)	61%	12%	2%	25%
Quebec	(168)	39%	38%	1%	22%
Ontario	(515)	64%	15%	1%	20%
Prairies	(652)	62%	16%	1%	21%
British Columbia	(424)	63%	16%	1%	21%
QD12 LANGUAGE					
English	(1999)	63%	16%	1%	21%
French	(153)	37%	40%	1%	22%

QS6 SPYWARE INFECTIONS COMP HAD IN PAST 6M

Approximately how many spyware infections has your home computer(s) had in the past 6 months?

	Total Respondents	1-3	4-10	11-25	26-100	100+	Don't know
TOTAL	(1326)	31%	18%	10%	12%	11%	19%
QD1 AGE GROUP							
18-24	(90)	28%	13%	12%	13%	16%	16%
25-34	(239)	36%	12%	13%	12%	9%	18%
35-44	(377)	32%	21%	10%	11%	9%	17%
45-54	(369)	30%	17%	10%	12%	11%	19%
55-64	(181)	30%	20%	6%	11%	11%	22%
65+	(67)	22%	24%	8%	8%	9%	29%
Refused	(3)	73%	0%	14%	0%	14%	0%
QD2 REGION CMA CA							
Newfoundland	(31)	28%	10%	11%	22%	10%	20%
Nova Scotia	(122)	26%	19%	10%	11%	13%	21%
New Brunswick	(73)	38%	14%	6%	12%	11%	18%
Prince Edward Island	(12)	19%	27%	0%	19%	11%	24%
Quebec	(68)	33%	23%	8%	8%	8%	20%
Ontario	(337)	29%	18%	11%	11%	12%	19%
Manitoba	(90)	33%	18%	8%	12%	9%	20%
Saskatchewan	(47)	38%	9%	6%	6%	14%	26%
Alberta	(284)	31%	14%	11%	12%	13%	19%
British Columbia	(262)	34%	17%	10%	16%	9%	15%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(116)	27%	15%	7%	14%	8%	28%
$25,000 To Less Than $50,000	(292)	36%	21%	9%	8%	11%	15%
$50,000 To Less Than $75,000	(308)	26%	22%	12%	13%	8%	20%
$75,000 And Over	(416)	31%	16%	10%	13%	14%	15%
Don't Know/Refused	(194)	34%	11%	9%	10%	9%	26%
QD3A PEOPLE IN HOUSEHOLD							
1	(192)	37%	22%	7%	8%	8%	19%
2	(427)	33%	16%	11%	12%	7%	22%
3	(264)	29%	19%	10%	12%	11%	19%
4	(284)	30%	16%	11%	15%	11%	17%
5	(107)	20%	16%	9%	12%	23%	20%
6	(50)	23%	26%	12%	8%	26%	6%
Refused	(2)	100%	0%	0%	0%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(821)	30%	17%	10%	12%	11%	20%
One	(173)	28%	16%	9%	13%	8%	26%
Two	(109)	26%	22%	15%	13%	17%	7%
Three	(26)	24%	16%	2%	25%	8%	25%
Four Or More	(7)	31%	10%	26%	15%	18%	0%
Refused	(147)	40%	17%	8%	7%	10%	18%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(815)	31%	17%	10%	12%	10%	20%
One	(188)	28%	17%	12%	11%	15%	17%
Two	(109)	23%	15%	11%	16%	15%	20%
Three	(21)	27%	33%	10%	10%	4%	15%
Four Or More	(3)	7%	0%	38%	0%	55%	0%
Refused	(147)	40%	17%	8%	7%	10%	18%
QD6 EDUCATION							
Elementary School	(16)	4%	37%	8%	15%	5%	31%
High School	(298)	31%	17%	8%	14%	12%	18%
Community College	(390)	29%	19%	11%	9%	13%	19%
University	(425)	35%	18%	11%	11%	7%	17%
Post-Graduate/Professionot Availablel	(193)	27%	13%	8%	14%	13%	25%
Don't Know/Refused	(4)	32%	57%	0%	0%	11%	0%
QD8 GENDER							
Male	(719)	33%	19%	9%	12%	12%	15%
Female	(607)	28%	17%	10%	10%	9%	25%
QD9 GENDERATION							
Male - 18 To 34	(176)	39%	9%	11%	13%	13%	15%
Male - 35 To 54	(379)	34%	23%	10%	12%	10%	11%
Male - 55+	(164)	27%	22%	7%	12%	12%	21%
Female - 18 To 34	(154)	27%	17%	15%	12%	8%	22%
Female - 35 To 54	(369)	28%	15%	10%	11%	11%	26%
Female - 55+	(84)	29%	20%	5%	9%	9%	27%
QD11 REGION							
Atlantic	(240)	29%	15%	8%	13%	11%	25%
Quebec	(66)	33%	24%	8%	9%	8%	18%
Ontario	(338)	29%	18%	11%	11%	12%	19%
Prairies	(420)	32%	14%	9%	11%	12%	21%
British Columbia	(262)	34%	17%	10%	15%	8%	16%
QD12 LANGUAGE							
English	(1268)	30%	17%	10%	12%	11%	20%
French	(58)	36%	23%	9%	7%	7%	17%

QS7 HOURS FIX SPYWARE INFECTIONS ON HOME COMP

On average, how many hours have you spent trying to fix spyware infections on your home computer(s) in the past 6 months?

	Total Respondents	1-5 hrs	5-10 hrs	10-25 hrs	25-100 hrs	100+ hrs	Not Available
TOTAL	(1326)	53%	19%	8%	2%	1%	17%
QD1 AGE GROUP							
18-24	(90)	49%	23%	8%	5%	2%	14%
25-34	(239)	61%	18%	8%	2%	0%	11%
35-44	(377)	49%	26%	8%	1%	2%	14%
45-54	(369)	58%	15%	11%	1%	0%	13%
55-64	(181)	46%	19%	6%	3%	0%	26%
65+	(67)	54%	11%	5%	0%	0%	31%
Refused	(3)	86%	0%	14%	0%	0%	0%
QD2 REGION CMA CA							
Newfoundland	(31)	62%	8%	26%	0%	2%	2%
Nova Scotia	(122)	48%	22%	7%	2%	0%	20%
New Brunswick	(73)	57%	23%	8%	1%	4%	7%
Prince Edward Island	(12)	57%	14%	0%	0%	11%	19%
Quebec	(68)	56%	25%	5%	2%	1%	11%
Ontario	(337)	53%	18%	7%	1%	0%	20%
Manitoba	(90)	47%	16%	7%	4%	0%	25%
Saskatchewan	(47)	48%	16%	11%	8%	0%	16%
Alberta	(284)	50%	20%	10%	2%	0%	19%
British Columbia	(262)	56%	18%	10%	3%	1%	13%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(116)	54%	16%	6%	2%	2%	20%
$25,000 To Less Than $50,000	(292)	49%	23%	9%	2%	0%	17%
$50,000 To Less Than $75,000	(308)	59%	16%	9%	2%	0%	15%
$75,000 And Over	(416)	54%	24%	7%	2%	1%	12%
Don't Know/Refused	(194)	51%	13%	8%	2%	1%	25%
QD3A PEOPLE IN HOUSEHOLD							
1	(192)	58%	17%	6%	0%	0%	19%
2	(427)	55%	18%	6%	2%	0%	19%
3	(264)	47%	21%	13%	2%	1%	16%
4	(284)	55%	15%	10%	4%	3%	14%
5	(107)	46%	31%	6%	1%	0%	15%
6	(50)	57%	33%	5%	1%	0%	5%
Refused	(2)	0%	0%	73%	0%	0%	27%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(821)	52%	20%	7%	3%	1%	17%
One	(173)	51%	16%	14%	1%	0%	18%
Two	(109)	54%	26%	10%	1%	0%	8%
Three	(26)	65%	11%	3%	4%	0%	17%
Four Or More	(7)	100%	0%	0%	0%	0%	0%
Refused	(147)	62%	10%	8%	0%	0%	19%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(815)	54%	19%	7%	2%	1%	18%
One	(188)	51%	23%	13%	2%	1%	11%
Two	(109)	45%	18%	13%	5%	4%	15%
Three	(21)	66%	27%	3%	0%	0%	3%
Four Or More	(3)	45%	55%	0%	0%	0%	0%
Refused	(147)	62%	10%	8%	0%	0%	19%
QD6 EDUCATION							
Elementary School	(16)	10%	38%	3%	0%	0%	49%
High School	(298)	53%	16%	10%	2%	1%	18%
Community College	(390)	55%	18%	7%	2%	1%	16%
University	(425)	52%	22%	7%	2%	0%	16%
Post-Graduate/Professionot Availablel	(193)	58%	19%	7%	2%	1%	13%
Don't Know/Refused	(4)	57%	0%	43%	0%	0%	0%
QD8 GENDER							
Male	(719)	57%	20%	6%	2%	1%	14%
Female	(607)	48%	19%	10%	2%	1%	21%
QD9 GENDERATION							
Male - 18 To 34	(176)	61%	21%	5%	2%	1%	10%
Male - 35 To 54	(379)	58%	21%	8%	1%	1%	10%
Male - 55+	(164)	53%	16%	5%	2%	0%	24%
Female - 18 To 34	(154)	54%	17%	11%	3%	0%	15%
Female - 35 To 54	(369)	48%	20%	11%	2%	1%	18%
Female - 55+	(84)	42%	18%	7%	2%	0%	31%
QD11 REGION							
Atlantic	(240)	53%	17%	10%	1%	2%	17%
Quebec	(66)	57%	26%	5%	2%	1%	9%
Ontario	(338)	53%	18%	7%	1%	0%	20%
Prairies	(420)	48%	19%	10%	4%	0%	20%
British Columbia	(262)	56%	18%	10%	3%	1%	13%
QD12 LANGUAGE							
English	(1268)	53%	18%	8%	2%	1%	18%
French	(58)	58%	25%	6%	2%	1%	8%

QS8 MONEY SPENT FIX SPYWARE ON HOME COMP

On average, how much money have you spent trying to fix spyware on your home computer(s) in the past 6 months?

	Total Respondents	0-$50	$51-100	$101-250	$250-1000	$1000+	Don't know
TOTAL	(1326)	60%	14%	7%	2%	0%	6%
QD1 AGE GROUP							
18-24	(90)	61%	13%	8%	2%	3%	6%
25-34	(239)	75%	7%	5%	1%	0%	5%
35-44	(377)	59%	14%	5%	3%	0%	8%
45-54	(369)	53%	17%	10%	2%	1%	6%
55-64	(181)	52%	16%	9%	1%	0%	6%
65+	(67)	58%	18%	7%	2%	0%	5%
Refused	(3)	73%	0%	0%	0%	0%	14%
QD2 REGION CMA CA							
Newfoundland	(31)	54%	25%	8%	0%	0%	5%
Nova Scotia	(122)	60%	13%	6%	2%	0%	8%
New Brunswick	(73)	73%	14%	6%	1%	0%	4%
Prince Edward Island	(12)	62%	0%	0%	8%	11%	0%
Quebec	(68)	59%	15%	8%	0%	0%	6%
Ontario	(337)	60%	12%	7%	2%	0%	8%
Manitoba	(90)	58%	19%	7%	2%	1%	4%
Saskatchewan	(47)	55%	18%	9%	5%	0%	4%
Alberta	(284)	55%	18%	8%	2%	2%	5%
British Columbia	(262)	63%	13%	8%	3%	1%	4%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(116)	70%	9%	3%	2%	0%	8%
$25,000 To Less Than $50,000	(292)	61%	14%	8%	1%	0%	3%
$50,000 To Less Than $75,000	(308)	63%	14%	4%	3%	1%	6%
$75,000 And Over	(416)	55%	18%	9%	2%	0%	6%
Don't Know/Refused	(194)	56%	8%	10%	1%	2%	13%
QD3A PEOPLE IN HOUSEHOLD							
1	(192)	66%	11%	4%	1%	0%	3%
2	(427)	62%	13%	8%	1%	1%	5%
3	(264)	57%	12%	7%	4%	0%	10%
4	(284)	55%	14%	8%	3%	1%	9%
5	(107)	53%	25%	8%	0%	1%	7%
6	(50)	62%	18%	9%	1%	0%	0%
Refused	(2)	0%	0%	73%	0%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(821)	58%	14%	8%	2%	1%	6%
One	(173)	55%	20%	5%	1%	0%	11%
Two	(109)	66%	9%	9%	3%	1%	5%
Three	(26)	76%	2%	5%	0%	0%	17%
Four Or More	(7)	69%	31%	0%	0%	0%	0%
Refused	(147)	65%	12%	5%	1%	0%	4%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(815)	61%	14%	7%	2%	1%	7%
One	(188)	59%	16%	8%	2%	1%	5%
Two	(109)	43%	19%	10%	5%	0%	14%
Three	(21)	71%	10%	16%	0%	0%	0%
Four Or More	(3)	7%	0%	55%	0%	0%	0%
Refused	(147)	65%	12%	5%	1%	0%	4%
QD6 EDUCATION							
Elementary School	(16)	57%	22%	0%	6%	0%	13%
High School	(298)	61%	12%	6%	2%	1%	7%
Community College	(390)	61%	12%	7%	2%	0%	5%
University	(425)	61%	13%	9%	2%	1%	7%
Post-Graduate/Professionot Availablel	(193)	53%	23%	7%	2%	0%	5%
Don't Know/Refused	(4)	68%	0%	32%	0%	0%	0%
QD8 GENDER							
Male	(719)	64%	14%	7%	2%	0%	4%
Female	(607)	54%	14%	8%	2%	1%	9%
QD9 GENDERATION							
Male - 18 To 34	(176)	77%	6%	6%	2%	1%	3%
Male - 35 To 54	(379)	60%	18%	8%	2%	0%	4%
Male - 55+	(164)	55%	16%	7%	2%	0%	6%
Female - 18 To 34	(154)	63%	14%	6%	1%	0%	9%
Female - 35 To 54	(369)	50%	12%	7%	3%	1%	12%
Female - 55+	(84)	52%	17%	10%	0%	1%	5%
QD11 REGION							
Atlantic	(240)	61%	14%	6%	2%	0%	5%
Quebec	(66)	61%	15%	8%	0%	0%	6%
Ontario	(338)	60%	12%	7%	2%	1%	8%
Prairies	(420)	55%	18%	8%	3%	2%	5%
British Columbia	(262)	64%	12%	8%	3%	0%	4%
QD12 LANGUAGE							
English	(1268)	59%	14%	7%	2%	1%	6%
French	(58)	63%	12%	10%	0%	0%	7%

{sh (Continued)}

QS8 MONEY SPENT FIX SPYWARE ON HOME COMP

On average, how much money have you spent trying to fix spyware on your home computer(s) in the past 6 months?

	Not applicable
TOTAL	10%
QD1 AGE GROUP	
18-24	9%
25-34	5%
35-44	11%
45-54	11%
55-64	15%
65+	10%
Refused	14%
QD2 REGION CMA CA	
Newfoundland	7%
Nova Scotia	11%
New Brunswick	2%
Prince Edward Island	19%
Quebec	12%
Ontario	11%
Manitoba	8%
Saskatchewan	10%
Alberta	10%
British Columbia	8%
QD3 HOUSEHOLD INCOME	
Less Than $25,000	7%
$25,000 To Less Than $50,000	13%
$50,000 To Less Than $75,000	11%
$75,000 And Over	9%
Don't Know/Refused	11%
QD3A PEOPLE IN HOUSEHOLD	
1	15%
2	10%
3	10%
4	9%
5	6%
6	10%
Refused	27%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE	
None	11%
One	7%
Two	7%
Three	0%
Four Or More	0%
Refused	13%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE	
None	10%
One	8%
Two	9%
Three	4%
Four Or More	38%
Refused	13%
QD6 EDUCATION	
Elementary School	1%
High School	12%
Community College	13%
University	8%
Post-Graduate/Professionot Availablel	10%
Don't Know/Refused	0%
QD8 GENDER	
Male	9%
Female	13%
QD9 GENDERATION	
Male - 18 To 34	6%
Male - 35 To 54	9%
Male - 55+	13%
Female - 18 To 34	7%
Female - 35 To 54	14%
Female - 55+	16%
QD11 REGION	
Atlantic	13%
Quebec	10%
Ontario	11%
Prairies	9%
British Columbia	8%
QD12 LANGUAGE	
English	11%
French	8%

QS9 SUCCESS IN REMOVING/FIX PROBLEM

Were you successful in removing or fixing the problem?

	Total Respondents	Yes	Partially successful	Don't know
TOTAL	(1326)	71%	23%	6%
QD1 AGE GROUP				
18-24	(90)	57%	41%	2%
25-34	(239)	71%	23%	6%
35-44	(377)	74%	23%	3%
45-54	(369)	71%	26%	4%
55-64	(181)	69%	19%	12%
65+	(67)	85%	11%	4%
Refused	(3)	100%	0%	0%
QD2 REGION CMA CA				
Newfoundland	(31)	79%	21%	0%
Nova Scotia	(122)	70%	28%	3%
New Brunswick	(73)	71%	23%	6%
Prince Edward Island	(12)	70%	30%	0%
Quebec	(68)	61%	38%	1%
Ontario	(337)	73%	19%	8%
Manitoba	(90)	74%	21%	6%
Saskatchewan	(47)	74%	19%	7%
Alberta	(284)	75%	18%	7%
British Columbia	(262)	74%	21%	5%
QD3 HOUSEHOLD INCOME				
Less Than $25,000	(116)	58%	31%	10%
$25,000 To Less Than $50,000	(292)	73%	22%	5%
$50,000 To Less Than $75,000	(308)	69%	25%	7%
$75,000 And Over	(416)	74%	21%	4%
Don't Know/Refused	(194)	74%	21%	5%
QD3A PEOPLE IN HOUSEHOLD				
1	(192)	74%	18%	8%
2	(427)	74%	20%	6%
3	(264)	72%	24%	4%
4	(284)	66%	28%	6%
5	(107)	62%	35%	3%
6	(50)	70%	25%	5%
Refused	(2)	100%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE				
None	(821)	71%	24%	5%
One	(173)	67%	29%	4%
Two	(109)	72%	24%	3%
Three	(26)	74%	16%	10%
Four Or More	(7)	83%	0%	17%
Refused	(147)	79%	13%	9%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE				
None	(815)	73%	21%	6%
One	(188)	62%	36%	1%
Two	(109)	66%	28%	6%
Three	(21)	73%	20%	7%
Four Or More	(3)	0%	100%	0%
Refused	(147)	79%	13%	9%
QD6 EDUCATION				
Elementary School	(16)	27%	41%	32%
High School	(298)	71%	23%	6%
Community College	(390)	73%	22%	6%
University	(425)	69%	27%	5%
Post-Graduate/Professionot Availablel	(193)	76%	18%	6%
Don't Know/Refused	(4)	100%	0%	0%
QD8 GENDER				
Male	(719)	75%	22%	3%
Female	(607)	66%	25%	9%
QD9 GENDERATION				
Male - 18 To 34	(176)	73%	24%	4%
Male - 35 To 54	(379)	74%	24%	2%
Male - 55+	(164)	79%	16%	5%
Female - 18 To 34	(154)	59%	34%	7%
Female - 35 To 54	(369)	70%	24%	6%
Female - 55+	(84)	65%	17%	17%
QD11 REGION				
Atlantic	(240)	72%	25%	3%
Quebec	(66)	60%	39%	1%
Ontario	(338)	73%	19%	8%
Prairies	(420)	74%	19%	6%
British Columbia	(262)	75%	20%	5%
QD12 LANGUAGE				
English	(1268)	74%	20%	6%
French	(58)	55%	44%	1%

QS10 HELP FROM FRIEND/TECH TO FIX PROBLEM

Did you require help from a friend or technician to fix the problem?

	Total Respondents	Yes	For some problems	Don't know
TOTAL	(1326)	90%	8%	2%
QD1 AGE GROUP				
18-24	(90)	80%	19%	1%
25-34	(239)	92%	6%	2%
35-44	(377)	88%	11%	1%
45-54	(369)	92%	7%	1%
55-64	(181)	92%	5%	3%
65+	(67)	94%	2%	4%
Refused	(3)	86%	14%	0%
QD2 REGION CMA CA				
Newfoundland	(31)	95%	5%	0%
Nova Scotia	(122)	92%	8%	0%
New Brunswick	(73)	84%	16%	0%
Prince Edward Island	(12)	89%	11%	0%
Quebec	(68)	93%	7%	0%
Ontario	(337)	88%	8%	3%
Manitoba	(90)	93%	5%	2%
Saskatchewan	(47)	77%	22%	1%
Alberta	(284)	88%	10%	1%
British Columbia	(262)	94%	5%	1%
QD3 HOUSEHOLD INCOME				
Less Than $25,000	(116)	90%	9%	1%
$25,000 To Less Than $50,000	(292)	91%	8%	0%
$50,000 To Less Than $75,000	(308)	91%	6%	3%
$75,000 And Over	(416)	88%	9%	2%
Don't Know/Refused	(194)	90%	9%	1%
QD3A PEOPLE IN HOUSEHOLD				
1	(192)	89%	10%	1%
2	(427)	92%	6%	2%
3	(264)	90%	8%	2%
4	(284)	87%	10%	2%
5	(107)	89%	8%	2%
6	(50)	92%	8%	0%
Refused	(2)	100%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE				
None	(821)	90%	8%	2%
One	(173)	91%	6%	2%
Two	(109)	89%	9%	2%
Three	(26)	86%	4%	10%
Four Or More	(7)	100%	0%	0%
Refused	(147)	88%	11%	2%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE				
None	(815)	91%	7%	2%
One	(188)	89%	10%	1%
Two	(109)	87%	11%	2%
Three	(21)	92%	8%	0%
Four Or More	(3)	93%	7%	0%
Refused	(147)	88%	11%	2%
QD6 EDUCATION				
Elementary School	(16)	78%	22%	0%
High School	(298)	87%	10%	3%
Community College	(390)	92%	7%	2%
University	(425)	91%	8%	1%
Post-Graduate/Professionot Availablel	(193)	91%	7%	2%
Don't Know/Refused	(4)	75%	25%	0%
QD8 GENDER				
Male	(719)	92%	7%	1%
Female	(607)	87%	10%	3%
QD9 GENDERATION				
Male - 18 To 34	(176)	92%	7%	0%
Male - 35 To 54	(379)	91%	8%	1%
Male - 55+	(164)	94%	5%	1%
Female - 18 To 34	(154)	82%	14%	3%
Female - 35 To 54	(369)	88%	11%	1%
Female - 55+	(84)	90%	5%	6%
QD11 REGION				
Atlantic	(240)	91%	9%	0%
Quebec	(66)	93%	7%	0%
Ontario	(338)	88%	9%	3%
Prairies	(420)	87%	11%	2%
British Columbia	(262)	94%	4%	1%
QD12 LANGUAGE				
English	(1268)	90%	8%	2%
French	(58)	93%	7%	0%

QS11_A USE ANTI-SPYWARE IN LAST 6M

Did you use an anti-spyware software product on your home computer(s) in the last 6 months?

	Total Respondents	Yes	Don't know
TOTAL	(2152)	91%	9%
QD1 AGE GROUP			
18-24	(132)	87%	13%
25-34	(369)	91%	9%
35-44	(566)	93%	7%
45-54	(593)	92%	8%
55-64	(345)	89%	11%
65+	(136)	92%	8%
Refused	(11)	94%	6%
QD2 REGION CMA CA			
Newfoundland	(47)	93%	7%
Nova Scotia	(192)	88%	12%
New Brunswick	(135)	87%	13%
Prince Edward Island	(18)	92%	8%
Quebec	(169)	93%	7%
Ontario	(516)	91%	9%
Manitoba	(142)	89%	11%
Saskatchewan	(74)	90%	10%
Alberta	(437)	92%	8%
British Columbia	(422)	90%	10%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	93%	7%
$25,000 To Less Than $50,000	(492)	89%	11%
$50,000 To Less Than $75,000	(488)	92%	8%
$75,000 And Over	(659)	92%	8%
Don't Know/Refused	(321)	91%	9%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	92%	8%
2	(749)	91%	9%
3	(424)	91%	9%
4	(433)	90%	10%
5	(159)	91%	9%
6	(83)	91%	9%
Refused	(3)	100%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	91%	9%
One	(262)	92%	8%
Two	(189)	88%	12%
Three	(40)	86%	14%
Four Or More	(11)	86%	14%
Refused	(218)	91%	9%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	91%	9%
One	(275)	93%	7%
Two	(151)	89%	11%
Three	(34)	96%	4%
Four Or More	(6)	90%	10%
Refused	(218)	91%	9%
QD6 EDUCATION			
Elementary School	(26)	99%	1%
High School	(497)	90%	10%
Community College	(615)	90%	10%
University	(685)	92%	8%
Post-Graduate/Professionot Availablel	(324)	91%	9%
Don't Know/Refused	(5)	100%	0%
QD8 GENDER			
Male	(1029)	96%	4%
Female	(1123)	87%	13%
QD9 GENDERATION			
Male - 18 To 34	(223)	97%	3%
Male - 35 To 54	(529)	96%	4%
Male - 55+	(277)	94%	6%
Female - 18 To 34	(280)	84%	16%
Female - 35 To 54	(637)	89%	11%
Female - 55+	(206)	87%	13%
QD11 REGION			
Atlantic	(393)	90%	10%
Quebec	(168)	92%	8%
Ontario	(515)	91%	9%
Prairies	(652)	91%	9%
British Columbia	(424)	91%	9%
QD12 LANGUAGE			
English	(1999)	91%	9%
French	(153)	91%	9%

QS11 EFFECTIVE IN REMOVING SPYWARE

Was it effective in removing the spyware?

	Total Respondents	Yes	Partially	Don't Know
TOTAL	(1748)	54%	20%	26%
QD1 AGE GROUP				
18-24	(108)	47%	32%	21%
25-34	(302)	56%	23%	21%
35-44	(463)	60%	19%	21%
45-54	(495)	57%	22%	22%
55-64	(264)	47%	14%	38%
65+	(107)	55%	9%	36%
Refused	(9)	51%	0%	49%
QD2 REGION CMA CA				
Newfoundland	(35)	68%	21%	11%
Nova Scotia	(162)	51%	24%	25%
New Brunswick	(107)	58%	16%	26%
Prince Edward Island	(13)	67%	12%	21%
Quebec	(118)	49%	21%	30%
Ontario	(426)	53%	20%	27%
Manitoba	(118)	58%	20%	23%
Saskatchewan	(65)	56%	14%	29%
Alberta	(356)	57%	19%	24%
British Columbia	(348)	59%	18%	22%
QD3 HOUSEHOLD INCOME				
Less Than $25,000	(153)	51%	18%	31%
$25,000 To Less Than $50,000	(379)	52%	17%	31%
$50,000 To Less Than $75,000	(403)	57%	22%	21%
$75,000 And Over	(547)	54%	21%	25%
Don't Know/Refused	(266)	56%	18%	27%
QD3A PEOPLE IN HOUSEHOLD				
1	(224)	54%	17%	29%
2	(597)	57%	16%	27%
3	(349)	53%	20%	27%
4	(371)	51%	25%	24%
5	(135)	49%	29%	22%
6	(70)	56%	17%	27%
Refused	(2)	27%	73%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE				
None	(1098)	53%	21%	26%
One	(228)	61%	15%	24%
Two	(159)	56%	19%	26%
Three	(34)	57%	19%	24%
Four Or More	(9)	76%	0%	24%
Refused	(167)	56%	16%	28%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE				
None	(1128)	56%	17%	27%
One	(233)	52%	32%	17%
Two	(130)	46%	24%	30%
Three	(31)	75%	16%	9%
Four Or More	(6)	0%	51%	49%
Refused	(167)	56%	16%	28%
QD6 EDUCATION				
Elementary School	(20)	56%	29%	15%
High School	(407)	55%	16%	29%
Community College	(528)	52%	20%	28%
University	(541)	54%	25%	21%
Post-Graduate/Professionot Availablel	(248)	57%	12%	31%
Don't Know/Refused	(4)	68%	32%	0%
QD8 GENDER				
Male	(842)	64%	21%	16%
Female	(906)	45%	18%	37%
QD9 GENDERATION				
Male - 18 To 34	(188)	64%	28%	8%
Male - 35 To 54	(441)	65%	22%	12%
Male - 55+	(213)	61%	11%	28%
Female - 18 To 34	(224)	43%	23%	34%
Female - 35 To 54	(522)	51%	18%	31%
Female - 55+	(160)	40%	14%	46%
QD11 REGION				
Atlantic	(318)	59%	20%	21%
Quebec	(117)	48%	21%	31%
Ontario	(425)	54%	19%	27%
Prairies	(539)	57%	20%	24%
British Columbia	(349)	60%	18%	23%
QD12 LANGUAGE				
English	(1644)	56%	19%	25%
French	(104)	44%	23%	33%

QS11B HOW MUCH PAY FOR THE SOFTWARE

On total, how much did you pay for the software?

	Total Respondents	1-$20	$20-$50	$51-$100	$101-$200	$200+	free download or illegal download copy
TOTAL	(1748)	8%	14%	12%	3%	1%	41%
QD1 AGE GROUP							
18-24	(108)	9%	12%	3%	4%	1%	44%
25-34	(302)	7%	10%	8%	1%	2%	55%
35-44	(463)	8%	15%	15%	3%	0%	41%
45-54	(495)	10%	13%	16%	5%	2%	35%
55-64	(264)	5%	16%	9%	2%	1%	38%
65+	(107)	8%	19%	18%	3%	0%	31%
Refused	(9)	0%	4%	23%	0%	0%	33%
QD2 REGION CMA CA							
Newfoundland	(35)	7%	16%	12%	2%	0%	51%
Nova Scotia	(162)	12%	10%	13%	4%	0%	36%
New Brunswick	(107)	9%	14%	9%	1%	3%	44%
Prince Edward Island	(13)	17%	2%	0%	0%	7%	50%
Quebec	(118)	8%	12%	12%	4%	0%	39%
Ontario	(426)	5%	14%	11%	3%	2%	43%
Manitoba	(118)	12%	11%	11%	2%	0%	41%
Saskatchewan	(65)	5%	7%	16%	0%	0%	48%
Alberta	(356)	10%	15%	14%	2%	0%	38%
British Columbia	(348)	10%	17%	12%	3%	1%	40%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(153)	8%	7%	13%	2%	1%	49%
$25,000 To Less Than $50,000	(379)	7%	13%	10%	2%	1%	41%
$50,000 To Less Than $75,000	(403)	10%	14%	10%	3%	1%	45%
$75,000 And Over	(547)	6%	16%	16%	4%	1%	38%
Don't Know/Refused	(266)	7%	15%	9%	3%	2%	38%
QD3A PEOPLE IN HOUSEHOLD							
1	(224)	10%	11%	11%	1%	1%	45%
2	(597)	6%	16%	11%	2%	1%	42%
3	(349)	7%	11%	13%	3%	1%	41%
4	(371)	8%	14%	14%	2%	1%	39%
5	(135)	6%	14%	15%	2%	0%	40%
6	(70)	9%	14%	7%	15%	0%	33%
Refused	(2)	0%	0%	0%	0%	0%	27%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1098)	6%	15%	12%	3%	1%	41%
One	(228)	7%	13%	16%	3%	2%	37%
Two	(159)	13%	12%	11%	1%	1%	44%
Three	(34)	9%	16%	3%	1%	0%	52%
Four Or More	(9)	0%	5%	0%	31%	0%	41%
Refused	(167)	14%	13%	12%	1%	1%	37%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1128)	7%	15%	11%	2%	1%	41%
One	(233)	6%	10%	17%	2%	1%	47%
Two	(130)	7%	12%	18%	4%	0%	32%
Three	(31)	16%	18%	13%	22%	0%	20%
Four Or More	(6)	3%	0%	0%	48%	0%	20%
Refused	(167)	14%	13%	12%	1%	1%	37%
QD6 EDUCATION							
Elementary School	(20)	4%	3%	17%	16%	3%	35%
High School	(407)	8%	16%	12%	2%	1%	35%
Community College	(528)	7%	15%	8%	3%	1%	45%
University	(541)	7%	10%	13%	3%	1%	44%
Post-Graduate/Professionot Availablel	(248)	8%	16%	17%	3%	0%	39%
Don't Know/Refused	(4)	32%	0%	0%	0%	0%	37%
QD8 GENDER							
Male	(842)	9%	14%	12%	3%	1%	49%
Female	(906)	6%	13%	12%	3%	0%	34%
QD9 GENDERATION							
Male - 18 To 34	(188)	7%	8%	5%	2%	3%	66%
Male - 35 To 54	(441)	11%	13%	16%	4%	1%	44%
Male - 55+	(213)	9%	22%	11%	2%	1%	39%
Female - 18 To 34	(224)	8%	14%	8%	2%	0%	38%
Female - 35 To 54	(522)	7%	14%	15%	3%	1%	31%
Female - 55+	(160)	3%	12%	12%	2%	0%	34%
QD11 REGION							
Atlantic	(318)	10%	12%	11%	2%	1%	44%
Quebec	(117)	7%	12%	12%	4%	0%	39%
Ontario	(425)	6%	14%	11%	3%	2%	43%
Prairies	(539)	10%	12%	13%	2%	0%	41%
British Columbia	(349)	10%	17%	12%	2%	0%	39%
QD12 LANGUAGE							
English	(1644)	8%	14%	12%	2%	1%	41%
French	(104)	6%	11%	12%	5%	0%	41%

{sh (Continued)}

QS11B HOW MUCH PAY FOR THE SOFTWARE

On total, how much did you pay for the software?

	Don't know
TOTAL	22%
QD1 AGE GROUP	
18-24	27%
25-34	16%
35-44	18%
45-54	21%
55-64	29%
65+	22%
Refused	40%
QD2 REGION CMA CA	
Newfoundland	12%
Nova Scotia	24%
New Brunswick	22%
Prince Edward Island	24%
Quebec	25%
Ontario	22%
Manitoba	24%
Saskatchewan	25%
Alberta	19%
British Columbia	18%
QD3 HOUSEHOLD INCOME	
Less Than $25,000	19%
$25,000 To Less Than $50,000	26%
$50,000 To Less Than $75,000	17%
$75,000 And Over	20%
Don't Know/Refused	26%
QD3A PEOPLE IN HOUSEHOLD	
1	21%
2	21%
3	23%
4	21%
5	22%
6	22%
Refused	73%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE	
None	22%
One	21%
Two	19%
Three	19%
Four Or More	23%
Refused	22%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE	
None	22%
One	18%
Two	27%
Three	11%
Four Or More	29%
Refused	22%
QD6 EDUCATION	
Elementary School	21%
High School	25%
Community College	21%
University	23%
Post-Graduate/Professionot Availablel	17%
Don't Know/Refused	32%
QD8 GENDER	
Male	12%
Female	32%
QD9 GENDERATION	
Male - 18 To 34	9%
Male - 35 To 54	11%
Male - 55+	16%
Female - 18 To 34	30%
Female - 35 To 54	29%
Female - 55+	37%
QD11 REGION	
Atlantic	20%
Quebec	25%
Ontario	21%
Prairies	22%
British Columbia	18%
QD12 LANGUAGE	
English	21%
French	25%

QS12A PROGRAM TRACKS WEATHER ON DESKTOP

Would you be willing to download a program that tracks the webpages you view and delivers popups to your home computer(s) in exchange for...A program that tracks local weather conditions on your desktop?

	Total Respondents	Yes	No
TOTAL	(2152)	10%	90%
QD1 AGE GROUP			
18-24	(132)	12%	88%
25-34	(369)	8%	92%
35-44	(566)	8%	92%
45-54	(593)	11%	89%
55-64	(345)	11%	89%
65+	(136)	13%	87%
Refused	(11)	4%	96%
QD2 REGION CMA CA			
Newfoundland	(47)	10%	90%
Nova Scotia	(192)	12%	88%
New Brunswick	(135)	5%	95%
Prince Edward Island	(18)	2%	98%
Quebec	(169)	16%	84%
Ontario	(516)	9%	91%
Manitoba	(142)	6%	94%
Saskatchewan	(74)	4%	96%
Alberta	(437)	9%	91%
British Columbia	(422)	4%	96%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	12%	88%
$25,000 To Less Than $50,000	(492)	12%	88%
$50,000 To Less Than $75,000	(488)	12%	88%
$75,000 And Over	(659)	9%	91%
Don't Know/Refused	(321)	5%	95%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	9%	91%
2	(749)	11%	89%
3	(424)	10%	90%
4	(433)	10%	90%
5	(159)	12%	88%
6	(83)	9%	91%
Refused	(3)	0%	100%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	11%	89%
One	(262)	8%	92%
Two	(189)	9%	91%
Three	(40)	4%	96%
Four Or More	(11)	5%	95%
Refused	(218)	8%	92%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	10%	90%
One	(275)	9%	91%
Two	(151)	11%	89%
Three	(34)	17%	83%
Four Or More	(6)	0%	100%
Refused	(218)	8%	92%
QD6 EDUCATION			
Elementary School	(26)	23%	77%
High School	(497)	12%	88%
Community College	(615)	12%	88%
University	(685)	8%	92%
Post-Graduate/Professionot Availablel	(324)	7%	93%
Don't Know/Refused	(5)	0%	100%
QD8 GENDER			
Male	(1029)	11%	89%
Female	(1123)	9%	91%
QD9 GENDERATION			
Male - 18 To 34	(223)	8%	92%
Male - 35 To 54	(529)	11%	89%
Male - 55+	(277)	12%	88%
Female - 18 To 34	(280)	9%	91%
Female - 35 To 54	(637)	8%	92%
Female - 55+	(206)	11%	89%
QD11 REGION			
Atlantic	(393)	9%	91%
Quebec	(168)	16%	84%
Ontario	(515)	9%	91%
Prairies	(652)	7%	93%
British Columbia	(424)	5%	95%
QD12 LANGUAGE			
English	(1999)	8%	92%
French	(153)	19%	81%

QS12B FILE SHARING PROGRAM

Would you be willing to download a program that tracks the webpages you view and delivers popups to your home computer(s) in exchange for...A file-sharing program?

	Total Respondents	Yes	No
TOTAL	(2152)	7%	93%
QD1 AGE GROUP			
18-24	(132)	13%	87%
25-34	(369)	10%	90%
35-44	(566)	7%	93%
45-54	(593)	6%	94%
55-64	(345)	4%	96%
65+	(136)	9%	91%
Refused	(11)	0%	100%
QD2 REGION CMA CA			
Newfoundland	(47)	8%	92%
Nova Scotia	(192)	9%	91%
New Brunswick	(135)	7%	93%
Prince Edward Island	(18)	8%	92%
Quebec	(169)	11%	89%
Ontario	(516)	6%	94%
Manitoba	(142)	6%	94%
Saskatchewan	(74)	4%	96%
Alberta	(437)	7%	93%
British Columbia	(422)	5%	95%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	11%	89%
$25,000 To Less Than $50,000	(492)	8%	92%
$50,000 To Less Than $75,000	(488)	8%	92%
$75,000 And Over	(659)	7%	93%
Don't Know/Refused	(321)	3%	97%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	6%	94%
2	(749)	5%	95%
3	(424)	9%	91%
4	(433)	10%	90%
5	(159)	9%	91%
6	(83)	8%	92%
Refused	(3)	0%	100%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	7%	93%
One	(262)	9%	91%
Two	(189)	10%	90%
Three	(40)	8%	92%
Four Or More	(11)	5%	95%
Refused	(218)	6%	94%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	7%	93%
One	(275)	14%	86%
Two	(151)	7%	93%
Three	(34)	2%	98%
Four Or More	(6)	0%	100%
Refused	(218)	6%	94%
QD6 EDUCATION			
Elementary School	(26)	17%	83%
High School	(497)	8%	92%
Community College	(615)	6%	94%
University	(685)	8%	92%
Post-Graduate/Professionot Availablel	(324)	5%	95%
Don't Know/Refused	(5)	27%	73%
QD8 GENDER			
Male	(1029)	7%	93%
Female	(1123)	7%	93%
QD9 GENDERATION			
Male - 18 To 34	(223)	11%	89%
Male - 35 To 54	(529)	8%	92%
Male - 55+	(277)	2%	98%
Female - 18 To 34	(280)	11%	89%
Female - 35 To 54	(637)	5%	95%
Female - 55+	(206)	7%	93%
QD11 REGION			
Atlantic	(393)	7%	93%
Quebec	(168)	11%	89%
Ontario	(515)	6%	94%
Prairies	(652)	7%	93%
British Columbia	(424)	6%	94%
QD12 LANGUAGE			
English	(1999)	6%	94%
French	(153)	12%	88%

QS12C SCREEN SAVER

Would you be willing to download a program that tracks the webpages you view and delivers popups to your home computer(s) in exchange for...A screen-saver?

	Total Respondents	Yes	No
TOTAL	(2152)	8%	92%
QD1 AGE GROUP			
18-24	(132)	12%	88%
25-34	(369)	7%	93%
35-44	(566)	6%	94%
45-54	(593)	8%	92%
55-64	(345)	10%	90%
65+	(136)	9%	91%
Refused	(11)	0%	100%
QD2 REGION CMA CA			
Newfoundland	(47)	4%	96%
Nova Scotia	(192)	7%	93%
New Brunswick	(135)	5%	95%
Prince Edward Island	(18)	16%	84%
Quebec	(169)	15%	85%
Ontario	(516)	6%	94%
Manitoba	(142)	7%	93%
Saskatchewan	(74)	10%	90%
Alberta	(437)	6%	94%
British Columbia	(422)	5%	95%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	11%	89%
$25,000 To Less Than $50,000	(492)	10%	90%
$50,000 To Less Than $75,000	(488)	12%	88%
$75,000 And Over	(659)	4%	96%
Don't Know/Refused	(321)	4%	96%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	5%	95%
2	(749)	9%	91%
3	(424)	9%	91%
4	(433)	8%	92%
5	(159)	10%	90%
6	(83)	11%	89%
Refused	(3)	0%	100%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	10%	90%
One	(262)	7%	93%
Two	(189)	11%	89%
Three	(40)	0%	100%
Four Or More	(11)	15%	85%
Refused	(218)	3%	97%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	9%	91%
One	(275)	10%	90%
Two	(151)	5%	95%
Three	(34)	5%	95%
Four Or More	(6)	20%	80%
Refused	(218)	3%	97%
QD6 EDUCATION			
Elementary School	(26)	19%	81%
High School	(497)	12%	88%
Community College	(615)	10%	90%
University	(685)	6%	94%
Post-Graduate/Professionot Availablel	(324)	4%	96%
Don't Know/Refused	(5)	0%	100%
QD8 GENDER			
Male	(1029)	7%	93%
Female	(1123)	9%	91%
QD9 GENDERATION			
Male - 18 To 34	(223)	6%	94%
Male - 35 To 54	(529)	6%	94%
Male - 55+	(277)	10%	90%
Female - 18 To 34	(280)	10%	90%
Female - 35 To 54	(637)	8%	92%
Female - 55+	(206)	10%	90%
QD11 REGION			
Atlantic	(393)	6%	94%
Quebec	(168)	15%	85%
Ontario	(515)	6%	94%
Prairies	(652)	7%	93%
British Columbia	(424)	5%	95%
QD12 LANGUAGE			
English	(1999)	6%	94%
French	(153)	16%	84%

QS12D PROGRAM ALLOWS ADD SMILEY FACES

Would you be willing to download a program that tracks the webpages you view and delivers popups to your home computer(s) in exchange for...A program that allows you to add smiley faces to your email or instant messenger?

	Total Respondents	Yes	No
TOTAL	(2152)	7%	93%
QD1 AGE GROUP			
18-24	(132)	10%	90%
25-34	(369)	7%	93%
35-44	(566)	6%	94%
45-54	(593)	9%	91%
55-64	(345)	6%	94%
65+	(136)	8%	92%
Refused	(11)	0%	100%
QD2 REGION CMA CA			
Newfoundland	(47)	4%	96%
Nova Scotia	(192)	6%	94%
New Brunswick	(135)	4%	96%
Prince Edward Island	(18)	10%	90%
Quebec	(169)	12%	88%
Ontario	(516)	5%	95%
Manitoba	(142)	5%	95%
Saskatchewan	(74)	4%	96%
Alberta	(437)	5%	95%
British Columbia	(422)	5%	95%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	14%	86%
$25,000 To Less Than $50,000	(492)	8%	92%
$50,000 To Less Than $75,000	(488)	8%	92%
$75,000 And Over	(659)	4%	96%
Don't Know/Refused	(321)	5%	95%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	5%	95%
2	(749)	7%	93%
3	(424)	7%	93%
4	(433)	8%	92%
5	(159)	11%	89%
6	(83)	5%	95%
Refused	(3)	0%	100%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	8%	92%
One	(262)	6%	94%
Two	(189)	7%	93%
Three	(40)	4%	96%
Four Or More	(11)	5%	95%
Refused	(218)	4%	96%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	7%	93%
One	(275)	7%	93%
Two	(151)	9%	91%
Three	(34)	5%	95%
Four Or More	(6)	20%	80%
Refused	(218)	4%	96%
QD6 EDUCATION			
Elementary School	(26)	21%	79%
High School	(497)	10%	90%
Community College	(615)	7%	93%
University	(685)	6%	94%
Post-Graduate/Professionot Availablel	(324)	5%	95%
Don't Know/Refused	(5)	0%	100%
QD8 GENDER			
Male	(1029)	5%	95%
Female	(1123)	9%	91%
QD9 GENDERATION			
Male - 18 To 34	(223)	4%	96%
Male - 35 To 54	(529)	6%	94%
Male - 55+	(277)	3%	97%
Female - 18 To 34	(280)	11%	89%
Female - 35 To 54	(637)	8%	92%
Female - 55+	(206)	8%	92%
QD11 REGION			
Atlantic	(393)	5%	95%
Quebec	(168)	12%	88%
Ontario	(515)	5%	95%
Prairies	(652)	5%	95%
British Columbia	(424)	6%	94%
QD12 LANGUAGE			
English	(1999)	5%	95%
French	(153)	14%	86%

QS13 ELEMNT OF PERS INFO TOLERATE OTHERS

Which elements of personal information would you tolerate others gathering?

	Total Respondents	Name	IP address	Other websites visited	What operating system you use	What programs you are running	What ISP you use
TOTAL	(341)	14%	3%	10%	6%	1%	5%
QD1 AGE GROUP							
18-24	(31)	12%	0%	19%	13%	0%	13%
25-34	(62)	13%	6%	8%	6%	1%	4%
35-44	(85)	12%	2%	4%	6%	0%	7%
45-54	(83)	18%	1%	7%	2%	2%	6%
55-64	(50)	13%	6%	16%	4%	2%	0%
65+	(29)	20%	0%	7%	11%	0%	0%
Refused	(1)	0%	0%	0%	100%	0%	0%
QD2 REGION CMA CA							
Newfoundland	(9)	8%	8%	8%	19%	0%	0%
Nova Scotia	(37)	7%	2%	16%	16%	5%	0%
New Brunswick	(19)	5%	0%	4%	5%	0%	4%
Prince Edward Island	(3)	44%	0%	0%	0%	0%	0%
Quebec	(46)	15%	2%	13%	4%	0%	9%
Ontario	(80)	14%	3%	8%	8%	1%	3%
Manitoba	(22)	21%	3%	30%	0%	0%	0%
Saskatchewan	(14)	12%	6%	0%	4%	0%	0%
Alberta	(62)	20%	7%	6%	3%	4%	4%
British Columbia	(49)	13%	2%	4%	9%	0%	0%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(44)	34%	0%	16%	7%	0%	3%
$25,000 To Less Than $50,000	(99)	10%	3%	7%	4%	1%	6%
$50,000 To Less Than $75,000	(82)	13%	4%	14%	6%	0%	5%
$75,000 And Over	(77)	13%	5%	6%	11%	1%	5%
Don't Know/Refused	(39)	4%	1%	6%	2%	4%	1%
QD3A PEOPLE IN HOUSEHOLD							
1	(48)	14%	2%	1%	3%	1%	9%
2	(102)	23%	4%	11%	5%	1%	1%
3	(66)	2%	5%	16%	9%	0%	5%
4	(76)	12%	1%	13%	5%	1%	8%
5	(32)	15%	4%	1%	10%	0%	8%
6	(17)	8%	0%	5%	7%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(211)	16%	2%	13%	7%	1%	4%
One	(39)	12%	15%	4%	8%	0%	1%
Two	(37)	10%	0%	5%	4%	1%	15%
Three	(6)	0%	0%	7%	9%	0%	0%
Four Or More	(2)	0%	0%	30%	0%	0%	0%
Refused	(33)	14%	3%	1%	4%	2%	5%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(213)	15%	4%	13%	6%	1%	4%
One	(46)	14%	3%	3%	8%	0%	4%
Two	(26)	8%	3%	10%	11%	0%	8%
Three	(8)	8%	0%	0%	17%	0%	20%
Four Or More	(2)	0%	0%	0%	0%	0%	0%
Refused	(33)	14%	3%	1%	4%	2%	5%
QD6 EDUCATION							
Elementary School	(5)	6%	0%	21%	0%	0%	0%
High School	(99)	19%	1%	19%	5%	1%	1%
Community College	(104)	16%	2%	4%	5%	2%	8%
University	(92)	9%	6%	5%	9%	0%	1%
Post-Graduate/Professionot Availablel	(40)	10%	3%	11%	9%	0%	13%
Don't Know/Refused	(1)	100%	0%	0%	0%	0%	0%
QD8 GENDER							
Male	(154)	15%	5%	7%	8%	1%	5%
Female	(187)	14%	2%	12%	5%	1%	4%
QD9 GENDERATION							
Male - 18 To 34	(33)	13%	7%	17%	8%	1%	7%
Male - 35 To 54	(73)	13%	3%	4%	5%	0%	8%
Male - 55+	(48)	18%	5%	3%	11%	1%	0%
Female - 18 To 34	(60)	12%	1%	8%	9%	0%	7%
Female - 35 To 54	(96)	18%	0%	7%	4%	2%	5%
Female - 55+	(31)	13%	3%	21%	1%	1%	0%
QD11 REGION							
Atlantic	(68)	9%	3%	10%	18%	2%	1%
Quebec	(45)	15%	2%	13%	4%	0%	9%
Ontario	(79)	14%	3%	8%	7%	1%	3%
Prairies	(99)	18%	6%	9%	2%	2%	2%
British Columbia	(50)	13%	1%	3%	8%	0%	0%
QD12 LANGUAGE							
English	(297)	14%	3%	8%	8%	1%	2%
French	(44)	15%	2%	14%	2%	0%	9%

{sh (Continued)}

QS13 ELEMNT OF PERS INFO TOLERATE OTHERS

Which elements of personal information would you tolerate others gathering?

	Which country accessing Internet from	Don't know
TOTAL	35%	26%
QD1 AGE GROUP		
18-24	19%	24%
25-34	46%	17%
35-44	30%	38%
45-54	38%	25%
55-64	34%	26%
65+	34%	28%
Refused	0%	0%
QD2 REGION CMA CA		
Newfoundland	39%	17%
Nova Scotia	35%	18%
New Brunswick	48%	34%
Prince Edward Island	56%	0%
Quebec	28%	29%
Ontario	37%	26%
Manitoba	29%	17%
Saskatchewan	44%	34%
Alberta	30%	26%
British Columbia	50%	22%
QD3 HOUSEHOLD INCOME		
Less Than $25,000	21%	19%
$25,000 To Less Than $50,000	36%	33%
$50,000 To Less Than $75,000	37%	22%
$75,000 And Over	33%	27%
Don't Know/Refused	49%	32%
QD3A PEOPLE IN HOUSEHOLD		
1	32%	39%
2	32%	23%
3	34%	28%
4	34%	26%
5	38%	24%
6	59%	21%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE		
None	34%	24%
One	29%	32%
Two	44%	21%
Three	74%	10%
Four Or More	70%	0%
Refused	40%	31%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE		
None	35%	22%
One	31%	36%
Two	31%	29%
Three	21%	34%
Four Or More	100%	0%
Refused	40%	31%
QD6 EDUCATION		
Elementary School	45%	28%
High School	28%	25%
Community College	32%	32%
University	49%	22%
Post-Graduate/Professionot Availablel	27%	27%
Don't Know/Refused	0%	0%
QD8 GENDER		
Male	30%	30%
Female	39%	24%
QD9 GENDERATION		
Male - 18 To 34	40%	8%
Male - 35 To 54	31%	36%
Male - 55+	20%	42%
Female - 18 To 34	34%	28%
Female - 35 To 54	37%	28%
Female - 55+	45%	15%
QD11 REGION		
Atlantic	37%	21%
Quebec	28%	29%
Ontario	36%	28%
Prairies	37%	24%
British Columbia	53%	21%
QD12 LANGUAGE		
English	39%	25%
French	28%	29%

QS14 FREQUENTLY TOLERATE VIEW POP-UPS

How frequently would you tolerate viewing pop-ups?

	Total Respondents	Every time I click a hyperlink	1-5 per computer use	1-10 a day	1-10 a week	1-10 a month	1-10 a year
TOTAL	(341)	1%	12%	4%	8%	9%	7%
QD1 AGE GROUP							
18-24	(31)	0%	13%	12%	15%	3%	6%
25-34	(62)	0%	15%	3%	8%	6%	10%
35-44	(85)	2%	11%	3%	7%	3%	12%
45-54	(83)	4%	8%	5%	12%	8%	0%
55-64	(50)	0%	5%	0%	3%	21%	3%
65+	(29)	1%	28%	4%	1%	12%	11%
Refused	(1)	0%	0%	0%	0%	100%	0%
QD2 REGION CMA CA							
Newfoundland	(9)	0%	0%	0%	0%	0%	28%
Nova Scotia	(37)	6%	10%	14%	5%	14%	6%
New Brunswick	(19)	0%	9%	4%	9%	5%	16%
Prince Edward Island	(3)	44%	0%	0%	0%	0%	11%
Quebec	(46)	2%	10%	2%	8%	11%	6%
Ontario	(80)	1%	18%	3%	5%	9%	3%
Manitoba	(22)	0%	5%	3%	18%	10%	17%
Saskatchewan	(14)	0%	0%	6%	7%	18%	19%
Alberta	(62)	0%	6%	5%	15%	5%	14%
British Columbia	(49)	0%	10%	8%	6%	9%	4%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(44)	0%	7%	8%	15%	1%	9%
$25,000 To Less Than $50,000	(99)	2%	16%	2%	4%	6%	7%
$50,000 To Less Than $75,000	(82)	1%	11%	5%	5%	17%	5%
$75,000 And Over	(77)	3%	10%	2%	13%	12%	7%
Don't Know/Refused	(39)	0%	11%	2%	0%	3%	9%
QD3A PEOPLE IN HOUSEHOLD							
1	(48)	0%	16%	3%	6%	7%	5%
2	(102)	2%	7%	4%	5%	16%	4%
3	(66)	0%	19%	2%	16%	1%	6%
4	(76)	4%	13%	8%	9%	10%	14%
5	(32)	0%	5%	0%	4%	8%	8%
6	(17)	0%	15%	3%	0%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(211)	2%	8%	4%	9%	12%	7%
One	(39)	0%	28%	2%	2%	3%	9%
Two	(37)	0%	13%	1%	8%	1%	6%
Three	(6)	0%	0%	0%	0%	0%	18%
Four Or More	(2)	0%	70%	30%	0%	0%	0%
Refused	(33)	0%	9%	3%	6%	11%	8%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(213)	2%	12%	4%	6%	10%	7%
One	(46)	0%	13%	8%	10%	13%	7%
Two	(26)	0%	2%	0%	20%	9%	11%
Three	(8)	0%	0%	0%	0%	0%	0%
Four Or More	(2)	0%	0%	0%	0%	0%	0%
Refused	(33)	0%	9%	3%	6%	11%	8%
QD6 EDUCATION							
Elementary School	(5)	0%	0%	21%	0%	0%	14%
High School	(99)	3%	17%	0%	9%	10%	4%
Community College	(104)	1%	7%	2%	6%	5%	6%
University	(92)	1%	16%	9%	7%	13%	9%
Post-Graduate/Professionot Availablel	(40)	0%	2%	2%	9%	13%	9%
Don't Know/Refused	(1)	0%	0%	0%	0%	0%	0%
QD8 GENDER							
Male	(154)	1%	13%	4%	7%	5%	6%
Female	(187)	1%	11%	3%	8%	14%	7%
QD9 GENDERATION							
Male - 18 To 34	(33)	0%	10%	6%	9%	2%	10%
Male - 35 To 54	(73)	2%	10%	6%	10%	2%	2%
Male - 55+	(48)	1%	20%	1%	2%	10%	8%
Female - 18 To 34	(60)	0%	18%	6%	11%	7%	8%
Female - 35 To 54	(96)	4%	9%	2%	10%	9%	10%
Female - 55+	(31)	0%	7%	1%	3%	24%	4%
QD11 REGION							
Atlantic	(68)	3%	7%	7%	4%	7%	13%
Quebec	(45)	2%	11%	2%	8%	10%	6%
Ontario	(79)	1%	18%	4%	5%	9%	3%
Prairies	(99)	1%	4%	3%	13%	9%	15%
British Columbia	(50)	0%	10%	7%	6%	13%	4%
QD12 LANGUAGE							
English	(297)	1%	12%	4%	7%	9%	7%
French	(44)	2%	11%	2%	8%	10%	6%

{sh (Continued)}

QS14 FREQUENTLY TOLERATE VIEW POP-UPS

How frequently would you tolerate viewing pop-ups?

	Never	Don't know
TOTAL	52%	8%
QD1 AGE GROUP		
18-24	44%	6%
25-34	45%	13%
35-44	51%	10%
45-54	57%	5%
55-64	61%	6%
65+	39%	5%
Refused	0%	0%
QD2 REGION CMA CA		
Newfoundland	53%	19%
Nova Scotia	27%	18%
New Brunswick	49%	8%
Prince Edward Island	44%	0%
Quebec	52%	9%
Ontario	55%	7%
Manitoba	43%	3%
Saskatchewan	37%	13%
Alberta	49%	5%
British Columbia	58%	5%
QD3 HOUSEHOLD INCOME		
Less Than $25,000	54%	6%
$25,000 To Less Than $50,000	45%	17%
$50,000 To Less Than $75,000	51%	5%
$75,000 And Over	53%	0%
Don't Know/Refused	68%	7%
QD3A PEOPLE IN HOUSEHOLD		
1	57%	6%
2	57%	5%
3	50%	5%
4	32%	9%
5	64%	12%
6	59%	23%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE		
None	52%	6%
One	52%	4%
Two	43%	28%
Three	82%	0%
Four Or More	0%	0%
Refused	53%	11%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE		
None	52%	8%
One	40%	9%
Two	56%	2%
Three	91%	9%
Four Or More	50%	50%
Refused	53%	11%
QD6 EDUCATION		
Elementary School	65%	0%
High School	50%	6%
Community College	58%	14%
University	43%	1%
Post-Graduate/Professionot Availablel	52%	13%
Don't Know/Refused	100%	0%
QD8 GENDER		
Male	56%	8%
Female	48%	8%
QD9 GENDERATION		
Male - 18 To 34	55%	9%
Male - 35 To 54	58%	9%
Male - 55+	53%	5%
Female - 18 To 34	37%	12%
Female - 35 To 54	50%	5%
Female - 55+	55%	6%
QD11 REGION		
Atlantic	44%	14%
Quebec	53%	9%
Ontario	53%	7%
Prairies	47%	6%
British Columbia	56%	4%
QD12 LANGUAGE		
English	51%	7%
French	52%	9%

QS15 READ LICENSE AGREEMENT WHEN DOWNLOAD

Do you read the license agreement when you legally download software?

	Total Respondents	Yes Always	Usually	Sometimes	No, Never	Don't Know
TOTAL	(2152)	20%	27%	35%	16%	2%
QD1 AGE GROUP						
18-24	(132)	15%	15%	38%	30%	2%
25-34	(369)	13%	28%	35%	23%	0%
35-44	(566)	17%	26%	36%	19%	2%
45-54	(593)	23%	28%	34%	14%	2%
55-64	(345)	25%	29%	35%	8%	3%
65+	(136)	23%	33%	29%	13%	3%
Refused	(11)	18%	42%	10%	18%	12%
QD2 REGION CMA CA						
Newfoundland	(47)	23%	39%	25%	10%	3%
Nova Scotia	(192)	18%	31%	35%	13%	2%
New Brunswick	(135)	20%	34%	31%	12%	2%
Prince Edward Island	(18)	16%	31%	37%	8%	8%
Quebec	(169)	17%	23%	41%	17%	1%
Ontario	(516)	21%	27%	32%	17%	2%
Manitoba	(142)	19%	26%	31%	17%	7%
Saskatchewan	(74)	13%	35%	37%	13%	2%
Alberta	(437)	21%	31%	31%	15%	2%
British Columbia	(422)	22%	29%	32%	15%	2%
QD3 HOUSEHOLD INCOME						
Less Than $25,000	(192)	21%	23%	40%	13%	2%
$25,000 To Less Than $50,000	(492)	20%	30%	30%	17%	2%
$50,000 To Less Than $75,000	(488)	17%	28%	38%	16%	2%
$75,000 And Over	(659)	17%	25%	37%	19%	2%
Don't Know/Refused	(321)	28%	28%	29%	12%	3%
QD3A PEOPLE IN HOUSEHOLD						
1	(301)	15%	33%	32%	18%	2%
2	(749)	23%	26%	33%	15%	2%
3	(424)	18%	28%	37%	16%	1%
4	(433)	17%	26%	38%	15%	4%
5	(159)	20%	22%	37%	19%	2%
6	(83)	20%	27%	29%	23%	1%
Refused	(3)	63%	37%	0%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE						
None	(1357)	21%	26%	35%	15%	2%
One	(262)	18%	31%	30%	18%	3%
Two	(189)	15%	24%	39%	19%	3%
Three	(40)	26%	22%	38%	15%	0%
Four Or More	(11)	0%	39%	37%	24%	0%
Refused	(218)	18%	35%	28%	18%	1%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE						
None	(1393)	20%	27%	35%	15%	2%
One	(275)	20%	25%	40%	13%	2%
Two	(151)	21%	24%	32%	22%	1%
Three	(34)	10%	37%	20%	33%	0%
Four Or More	(6)	23%	29%	28%	20%	0%
Refused	(218)	18%	35%	28%	18%	1%
QD6 EDUCATION						
Elementary School	(26)	19%	26%	44%	10%	0%
High School	(497)	24%	30%	29%	14%	3%
Community College	(615)	20%	27%	34%	17%	3%
University	(685)	17%	24%	41%	16%	2%
Post-Graduate/Professionot Availablel	(324)	18%	34%	30%	18%	0%
Don't Know/Refused	(5)	27%	0%	36%	37%	0%
QD8 GENDER						
Male	(1029)	17%	25%	37%	21%	1%
Female	(1123)	22%	30%	32%	12%	3%
QD9 GENDERATION						
Male - 18 To 34	(223)	15%	21%	36%	28%	0%
Male - 35 To 54	(529)	16%	24%	38%	20%	2%
Male - 55+	(277)	18%	30%	36%	15%	1%
Female - 18 To 34	(280)	11%	29%	36%	22%	2%
Female - 35 To 54	(637)	23%	30%	32%	13%	3%
Female - 55+	(206)	30%	31%	31%	4%	5%
QD11 REGION						
Atlantic	(393)	19%	33%	35%	11%	2%
Quebec	(168)	17%	24%	41%	18%	1%
Ontario	(515)	21%	27%	32%	17%	2%
Prairies	(652)	19%	30%	32%	15%	4%
British Columbia	(424)	22%	29%	32%	16%	2%
QD12 LANGUAGE						
English	(1999)	20%	29%	33%	16%	3%
French	(153)	18%	23%	40%	18%	0%

QS16 DESCRIBE EASE OF READING SOFTWARE

How would you describe the ease of reading a software licence agreement? Is it....

	Total Respondents	Easy	Manageable	Difficult	Incomprehensible	Don't know
TOTAL	(2152)	5%	35%	42%	13%	5%
QD1 AGE GROUP						
18-24	(132)	4%	42%	33%	15%	6%
25-34	(369)	3%	38%	40%	13%	7%
35-44	(566)	4%	37%	41%	14%	5%
45-54	(593)	3%	32%	49%	13%	3%
55-64	(345)	10%	32%	40%	12%	6%
65+	(136)	4%	33%	48%	11%	4%
Refused	(11)	0%	15%	54%	31%	0%
QD2 REGION CMA CA						
Newfoundland	(47)	0%	49%	36%	9%	6%
Nova Scotia	(192)	6%	37%	42%	10%	5%
New Brunswick	(135)	4%	31%	47%	14%	4%
Prince Edward Island	(18)	20%	27%	37%	16%	0%
Quebec	(169)	10%	32%	41%	11%	5%
Ontario	(516)	3%	37%	41%	14%	5%
Manitoba	(142)	3%	33%	41%	10%	12%
Saskatchewan	(74)	3%	34%	43%	14%	6%
Alberta	(437)	3%	33%	44%	14%	5%
British Columbia	(422)	2%	34%	43%	15%	5%
QD3 HOUSEHOLD INCOME						
Less Than $25,000	(192)	7%	38%	34%	13%	8%
$25,000 To Less Than $50,000	(492)	7%	35%	39%	13%	6%
$50,000 To Less Than $75,000	(488)	6%	30%	48%	12%	4%
$75,000 And Over	(659)	3%	39%	41%	12%	4%
Don't Know/Refused	(321)	2%	32%	45%	17%	5%
QD3A PEOPLE IN HOUSEHOLD						
1	(301)	11%	34%	36%	14%	5%
2	(749)	4%	36%	42%	13%	4%
3	(424)	4%	34%	47%	9%	7%
4	(433)	3%	35%	39%	15%	7%
5	(159)	5%	29%	46%	16%	4%
6	(83)	1%	39%	45%	11%	4%
Refused	(3)	0%	17%	83%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE						
None	(1357)	4%	37%	42%	13%	5%
One	(262)	3%	30%	50%	12%	5%
Two	(189)	3%	27%	45%	17%	8%
Three	(40)	3%	46%	35%	6%	9%
Four Or More	(11)	0%	34%	45%	8%	12%
Refused	(218)	10%	31%	39%	15%	5%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE						
None	(1393)	4%	36%	42%	12%	6%
One	(275)	4%	32%	44%	16%	5%
Two	(151)	3%	35%	44%	17%	2%
Three	(34)	0%	23%	71%	5%	1%
Four Or More	(6)	0%	49%	51%	0%	0%
Refused	(218)	10%	31%	39%	15%	5%
QD6 EDUCATION						
Elementary School	(26)	4%	40%	47%	8%	0%
High School	(497)	7%	39%	38%	11%	5%
Community College	(615)	2%	33%	43%	15%	7%
University	(685)	7%	31%	45%	13%	4%
Post-Graduate/Professionot Availablel	(324)	4%	40%	40%	14%	2%
Don't Know/Refused	(5)	0%	22%	27%	41%	10%
QD8 GENDER						
Male	(1029)	4%	33%	45%	15%	3%
Female	(1123)	6%	36%	39%	11%	7%
QD9 GENDERATION						
Male - 18 To 34	(223)	4%	37%	37%	18%	3%
Male - 35 To 54	(529)	4%	33%	47%	13%	3%
Male - 55+	(277)	2%	30%	50%	15%	2%
Female - 18 To 34	(280)	3%	40%	39%	9%	9%
Female - 35 To 54	(637)	2%	36%	43%	14%	5%
Female - 55+	(206)	13%	34%	35%	10%	8%
QD11 REGION						
Atlantic	(393)	5%	38%	43%	11%	4%
Quebec	(168)	10%	32%	41%	11%	5%
Ontario	(515)	3%	37%	41%	14%	5%
Prairies	(652)	3%	33%	43%	14%	7%
British Columbia	(424)	2%	34%	43%	15%	5%
QD12 LANGUAGE						
English	(1999)	3%	35%	42%	14%	6%
French	(153)	11%	34%	41%	11%	2%

QS17 MORE LIKELY TO READ LICENSE AGREEMENT

Would you be more likely to read the license agreement if it were:

	Total Respondents	Shorter & clearer	In standard format	Summarized the main points at the start	Sent to you to review later, by e-mail	Other	Don't know
TOTAL	(2152)	56%	7%	31%	1%	1%	4%
QD1 AGE GROUP							
18-24	(132)	56%	4%	36%	0%	2%	3%
25-34	(369)	59%	6%	28%	1%	2%	4%
35-44	(566)	55%	7%	33%	1%	0%	4%
45-54	(593)	56%	8%	31%	0%	0%	4%
55-64	(345)	53%	9%	32%	1%	1%	5%
65+	(136)	55%	6%	32%	2%	0%	4%
Refused	(11)	61%	11%	15%	0%	0%	12%
QD2 REGION CMA CA							
Newfoundland	(47)	69%	5%	22%	0%	0%	4%
Nova Scotia	(192)	48%	8%	37%	0%	1%	5%
New Brunswick	(135)	49%	4%	43%	1%	0%	4%
Prince Edward Island	(18)	57%	14%	27%	0%	0%	2%
Quebec	(169)	62%	5%	29%	0%	1%	3%
Ontario	(516)	54%	7%	33%	1%	1%	4%
Manitoba	(142)	52%	11%	32%	1%	1%	4%
Saskatchewan	(74)	58%	10%	28%	0%	0%	5%
Alberta	(437)	50%	8%	33%	2%	2%	5%
British Columbia	(422)	55%	10%	28%	1%	1%	5%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	57%	8%	26%	0%	4%	5%
$25,000 To Less Than $50,000	(492)	60%	7%	27%	1%	1%	4%
$50,000 To Less Than $75,000	(488)	55%	7%	33%	0%	0%	4%
$75,000 And Over	(659)	48%	7%	38%	1%	1%	5%
Don't Know/Refused	(321)	64%	6%	25%	1%	0%	3%
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	54%	11%	28%	1%	0%	6%
2	(749)	54%	6%	34%	1%	1%	3%
3	(424)	57%	5%	33%	1%	1%	3%
4	(433)	56%	8%	28%	1%	1%	6%
5	(159)	66%	9%	21%	0%	0%	4%
6	(83)	52%	6%	38%	1%	1%	2%
Refused	(3)	0%	0%	100%	0%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	55%	7%	33%	1%	1%	4%
One	(262)	66%	3%	28%	0%	0%	3%
Two	(189)	53%	8%	32%	1%	1%	5%
Three	(40)	60%	13%	21%	0%	0%	7%
Four Or More	(11)	64%	0%	36%	0%	0%	0%
Refused	(218)	57%	10%	25%	0%	0%	7%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	54%	6%	33%	1%	1%	4%
One	(275)	63%	10%	23%	0%	0%	4%
Two	(151)	66%	7%	26%	0%	0%	1%
Three	(34)	40%	18%	39%	2%	1%	0%
Four Or More	(6)	39%	3%	57%	0%	0%	0%
Refused	(218)	57%	10%	25%	0%	0%	7%
QD6 EDUCATION							
Elementary School	(26)	54%	14%	27%	0%	3%	2%
High School	(497)	65%	6%	24%	1%	1%	3%
Community College	(615)	62%	6%	26%	1%	0%	5%
University	(685)	47%	8%	40%	1%	1%	4%
Post-Graduate/Professionot Availablel	(324)	48%	8%	35%	1%	1%	6%
Don't Know/Refused	(5)	14%	22%	64%	0%	0%	0%
QD8 GENDER							
Male	(1029)	52%	9%	33%	1%	1%	4%
Female	(1123)	59%	6%	30%	1%	0%	4%
QD9 GENDERATION							
Male - 18 To 34	(223)	43%	8%	39%	1%	3%	5%
Male - 35 To 54	(529)	55%	11%	29%	1%	1%	4%
Male - 55+	(277)	56%	6%	32%	1%	0%	4%
Female - 18 To 34	(280)	74%	2%	21%	1%	0%	2%
Female - 35 To 54	(637)	56%	5%	35%	1%	0%	4%
Female - 55+	(206)	52%	10%	32%	1%	1%	5%
QD11 REGION							
Atlantic	(393)	51%	7%	38%	0%	0%	4%
Quebec	(168)	62%	5%	29%	0%	1%	3%
Ontario	(515)	54%	7%	33%	1%	1%	4%
Prairies	(652)	52%	9%	32%	1%	1%	5%
British Columbia	(424)	55%	9%	29%	1%	1%	5%
QD12 LANGUAGE							
English	(1999)	54%	8%	31%	1%	1%	5%
French	(153)	60%	6%	32%	0%	0%	2%

QD1 AGE GROUP

QD1 AGE GROUP

	Total Respondents	18-24	25-34	35-44	45-54	55-64	65+
TOTAL	(2152)	7%	19%	20%	21%	24%	8%
QD1 AGE GROUP							
18-24	(132)	100%	0%	0%	0%	0%	0%
25-34	(369)	0%	100%	0%	0%	0%	0%
35-44	(566)	0%	0%	100%	0%	0%	0%
45-54	(593)	0%	0%	0%	100%	0%	0%
55-64	(345)	0%	0%	0%	0%	100%	0%
65+	(136)	0%	0%	0%	0%	0%	100%
Refused	(11)	0%	0%	0%	0%	0%	0%
QD2 REGION CMA CA							
Newfoundland	(47)	6%	22%	17%	25%	25%	3%
Nova Scotia	(192)	5%	22%	18%	22%	26%	8%
New Brunswick	(135)	9%	19%	20%	21%	20%	11%
Prince Edward Island	(18)	0%	12%	33%	43%	10%	2%
Quebec	(169)	9%	17%	20%	19%	31%	4%
Ontario	(516)	7%	19%	20%	21%	22%	10%
Manitoba	(142)	9%	18%	21%	20%	22%	10%
Saskatchewan	(74)	7%	18%	17%	20%	30%	8%
Alberta	(437)	8%	21%	23%	21%	20%	6%
British Columbia	(422)	5%	22%	18%	21%	24%	9%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	24%	31%	16%	15%	10%	4%
$25,000 To Less Than $50,000	(492)	6%	21%	22%	12%	30%	9%
$50,000 To Less Than $75,000	(488)	5%	20%	21%	23%	25%	8%
$75,000 And Over	(659)	5%	16%	23%	26%	23%	8%
Don't Know/Refused	(321)	7%	13%	13%	26%	28%	9%
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	5%	16%	15%	17%	32%	14%
2	(749)	7%	17%	11%	16%	37%	13%
3	(424)	12%	23%	21%	23%	19%	1%
4	(433)	6%	22%	33%	27%	10%	1%
5	(159)	6%	22%	40%	26%	6%	1%
6	(83)	16%	18%	29%	28%	7%	3%
Refused	(3)	0%	0%	54%	46%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	9%	14%	14%	24%	30%	8%
One	(262)	4%	30%	43%	19%	2%	0%
Two	(189)	2%	43%	42%	11%	0%	0%
Three	(40)	0%	41%	50%	9%	0%	0%
Four Or More	(11)	4%	47%	26%	23%	0%	0%
Refused	(218)	5%	16%	18%	16%	29%	14%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	8%	23%	16%	17%	28%	8%
One	(275)	8%	11%	36%	37%	6%	2%
Two	(151)	6%	5%	48%	36%	5%	0%
Three	(34)	2%	0%	24%	61%	13%	0%
Four Or More	(6)	28%	0%	33%	20%	20%	0%
Refused	(218)	5%	16%	18%	16%	29%	14%
QD6 EDUCATION							
Elementary School	(26)	13%	0%	25%	30%	31%	0%
High School	(497)	15%	12%	15%	20%	28%	9%
Community College	(615)	7%	22%	25%	23%	20%	3%
University	(685)	4%	25%	20%	20%	24%	7%
Post-Graduate/Professionot Availablel	(324)	2%	15%	20%	19%	28%	16%
Don't Know/Refused	(5)	0%	0%	0%	86%	14%	0%
QD8 GENDER							
Male	(1029)	7%	21%	22%	21%	19%	10%
Female	(1123)	8%	18%	19%	20%	30%	6%
QD9 GENDERATION							
Male - 18 To 34	(223)	26%	74%	0%	0%	0%	0%
Male - 35 To 54	(529)	0%	0%	50%	49%	0%	0%
Male - 55+	(277)	0%	0%	0%	0%	65%	34%
Female - 18 To 34	(280)	30%	70%	0%	0%	0%	0%
Female - 35 To 54	(637)	0%	0%	48%	51%	0%	0%
Female - 55+	(206)	0%	0%	0%	0%	84%	16%
QD11 REGION							
Atlantic	(393)	6%	20%	19%	22%	26%	7%
Quebec	(168)	9%	17%	21%	19%	30%	4%
Ontario	(515)	7%	19%	21%	21%	22%	10%
Prairies	(652)	8%	19%	21%	21%	22%	8%
British Columbia	(424)	5%	22%	19%	21%	23%	9%
QD12 LANGUAGE							
English	(1999)	7%	19%	20%	20%	24%	9%
French	(153)	9%	18%	22%	22%	27%	2%

{sh (Continued)}

QD1 AGE GROUP

QD1 AGE GROUP

	Refused
TOTAL	0%
QD1 AGE GROUP	
18-24	0%
25-34	0%
35-44	0%
45-54	0%
55-64	0%
65+	0%
Refused	100%
QD2 REGION CMA CA	
Newfoundland	3%
Nova Scotia	0%
New Brunswick	1%
Prince Edward Island	0%
Quebec	0%
Ontario	1%
Manitoba	0%
Saskatchewan	0%
Alberta	1%
British Columbia	0%
QD3 HOUSEHOLD INCOME	
Less Than $25,000	0%
$25,000 To Less Than $50,000	0%
$50,000 To Less Than $75,000	0%
$75,000 And Over	0%
Don't Know/Refused	3%
QD3A PEOPLE IN HOUSEHOLD	
1	1%
2	0%
3	0%
4	1%
5	0%
6	0%
Refused	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE	
None	0%
One	1%
Two	1%
Three	0%
Four Or More	0%
Refused	1%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE	
None	0%
One	0%
Two	0%
Three	0%
Four Or More	0%
Refused	1%
QD6 EDUCATION	
Elementary School	0%
High School	0%
Community College	0%
University	0%
Post-Graduate/Professionot Availablel	1%
Don't Know/Refused	0%
QD8 GENDER	
Male	0%
Female	0%
QD9 GENDERATION	
Male - 18 To 34	1%
Male - 35 To 54	0%
Male - 55+	0%
Female - 18 To 34	0%
Female - 35 To 54	1%
Female - 55+	0%
QD11 REGION	
Atlantic	0%
Quebec	0%
Ontario	1%
Prairies	0%
British Columbia	1%
QD12 LANGUAGE	
English	1%
French	0%

QD2 REGION CMA CA

QD2 REGION CMA CA

	Total Respondents	Newfoundland	Nova Scotia	New Brunswick	Prince Edward Island	Quebec	Ontario
TOTAL	(2152)	2%	3%	2%	0%	25%	38%
QD1 AGE GROUP							
18-24	(132)	1%	2%	3%	0%	30%	37%
25-34	(369)	2%	3%	2%	0%	22%	38%
35-44	(566)	1%	3%	2%	1%	26%	38%
45-54	(593)	2%	3%	2%	1%	24%	38%
55-64	(345)	2%	3%	2%	0%	32%	33%
65+	(136)	1%	3%	3%	0%	13%	48%
Refused	(11)	11%	0%	3%	0%	0%	58%
QD2 REGION CMA CA							
Newfoundland	(47)	100%	0%	0%	0%	0%	0%
Nova Scotia	(192)	0%	100%	0%	0%	0%	0%
New Brunswick	(135)	0%	0%	100%	0%	0%	0%
Prince Edward Island	(18)	0%	0%	0%	100%	0%	0%
Quebec	(169)	0%	0%	0%	0%	100%	0%
Ontario	(516)	0%	0%	0%	0%	0%	100%
Manitoba	(142)	0%	0%	0%	0%	0%	0%
Saskatchewan	(74)	0%	0%	0%	0%	0%	0%
Alberta	(437)	0%	0%	0%	0%	0%	0%
British Columbia	(422)	0%	0%	0%	0%	0%	0%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	2%	3%	3%	0%	35%	33%
$25,000 To Less Than $50,000	(492)	2%	4%	2%	1%	34%	28%
$50,000 To Less Than $75,000	(488)	1%	3%	2%	0%	30%	36%
$75,000 And Over	(659)	1%	2%	2%	0%	15%	48%
Don't Know/Refused	(321)	2%	3%	4%	0%	18%	39%
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	1%	2%	2%	0%	35%	33%
2	(749)	2%	3%	2%	0%	24%	36%
3	(424)	1%	4%	3%	0%	22%	40%
4	(433)	2%	3%	2%	1%	19%	44%
5	(159)	3%	2%	4%	1%	32%	31%
6	(83)	1%	1%	1%	0%	29%	40%
Refused	(3)	0%	0%	0%	0%	0%	83%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	2%	3%	3%	0%	24%	38%
One	(262)	2%	4%	1%	1%	23%	36%
Two	(189)	1%	3%	3%	1%	24%	39%
Three	(40)	3%	1%	5%	4%	11%	43%
Four Or More	(11)	0%	0%	0%	0%	47%	33%
Refused	(218)	1%	3%	2%	0%	28%	37%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	2%	3%	2%	1%	22%	39%
One	(275)	3%	3%	4%	0%	25%	34%
Two	(151)	1%	2%	1%	0%	33%	37%
Three	(34)	4%	2%	3%	0%	30%	37%
Four Or More	(6)	0%	0%	0%	0%	67%	29%
Refused	(218)	1%	3%	2%	0%	28%	37%
QD6 EDUCATION							
Elementary School	(26)	3%	3%	4%	5%	29%	29%
High School	(497)	1%	3%	2%	0%	26%	37%
Community College	(615)	3%	3%	2%	1%	28%	34%
University	(685)	1%	3%	3%	0%	26%	37%
Post-Graduate/Professionot Availablel	(324)	3%	3%	1%	0%	20%	46%
Don't Know/Refused	(5)	0%	0%	0%	0%	0%	77%
QD8 GENDER							
Male	(1029)	2%	3%	2%	0%	25%	38%
Female	(1123)	2%	3%	2%	0%	26%	37%
QD9 GENDERATION							
Male - 18 To 34	(223)	1%	3%	3%	0%	24%	37%
Male - 35 To 54	(529)	2%	3%	2%	1%	25%	38%
Male - 55+	(277)	2%	4%	2%	0%	24%	37%
Female - 18 To 34	(280)	2%	3%	2%	0%	24%	38%
Female - 35 To 54	(637)	2%	3%	3%	1%	24%	38%
Female - 55+	(206)	2%	3%	2%	0%	30%	36%
QD11 REGION							
Atlantic	(393)	21%	38%	31%	5%	3%	1%
Quebec	(168)	0%	0%	0%	0%	100%	0%
Ontario	(515)	0%	0%	0%	0%	0%	99%
Prairies	(652)	0%	0%	0%	0%	0%	1%
British Columbia	(424)	0%	0%	0%	0%	1%	2%
QD12 LANGUAGE							
English	(1999)	2%	4%	3%	1%	5%	48%
French	(153)	0%	0%	0%	0%	100%	0%

{sh (Continued)}

QD2 REGION CMA CA

QD2 REGION CMA CA

	Manitoba	Saskatchewan	Alberta	British Columbia
TOTAL	4%	3%	9%	13%
QD1 AGE GROUP				
18-24	4%	3%	11%	10%
25-34	3%	3%	10%	15%
35-44	4%	3%	11%	12%
45-54	3%	3%	10%	14%
55-64	3%	4%	8%	13%
65+	5%	3%	8%	16%
Refused	0%	0%	17%	11%
QD2 REGION CMA CA				
Newfoundland	0%	0%	0%	0%
Nova Scotia	0%	0%	0%	0%
New Brunswick	0%	0%	0%	0%
Prince Edward Island	0%	0%	0%	0%
Quebec	0%	0%	0%	0%
Ontario	0%	0%	0%	0%
Manitoba	100%	0%	0%	0%
Saskatchewan	0%	100%	0%	0%
Alberta	0%	0%	100%	0%
British Columbia	0%	0%	0%	100%
QD3 HOUSEHOLD INCOME				
Less Than $25,000	3%	4%	7%	10%
$25,000 To Less Than $50,000	3%	3%	9%	14%
$50,000 To Less Than $75,000	4%	3%	8%	13%
$75,000 And Over	3%	4%	10%	13%
Don't Know/Refused	4%	2%	13%	14%
QD3A PEOPLE IN HOUSEHOLD				
1	3%	3%	9%	11%
2	4%	3%	10%	15%
3	4%	2%	10%	13%
4	3%	5%	9%	13%
5	3%	4%	9%	11%
6	2%	3%	10%	13%
Refused	0%	0%	0%	17%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE				
None	4%	3%	9%	14%
One	4%	3%	12%	14%
Two	4%	4%	10%	11%
Three	1%	2%	11%	19%
Four Or More	7%	0%	9%	4%
Refused	4%	5%	9%	11%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE				
None	4%	3%	10%	14%
One	3%	4%	11%	13%
Two	1%	4%	10%	10%
Three	1%	3%	6%	14%
Four Or More	0%	0%	3%	0%
Refused	4%	5%	9%	11%
QD6 EDUCATION				
Elementary School	8%	0%	16%	5%
High School	4%	4%	9%	14%
Community College	3%	3%	10%	14%
University	4%	4%	10%	11%
Post-Graduate/Professionot Availablel	2%	2%	9%	14%
Don't Know/Refused	0%	0%	0%	23%
QD8 GENDER				
Male	4%	3%	10%	13%
Female	3%	3%	9%	13%
QD9 GENDERATION				
Male - 18 To 34	4%	3%	11%	14%
Male - 35 To 54	3%	3%	10%	13%
Male - 55+	4%	5%	8%	14%
Female - 18 To 34	4%	3%	10%	13%
Female - 35 To 54	4%	3%	10%	13%
Female - 55+	3%	3%	7%	13%
QD11 REGION				
Atlantic	0%	0%	0%	1%
Quebec	0%	0%	0%	0%
Ontario	0%	0%	0%	0%
Prairies	22%	19%	57%	1%
British Columbia	0%	0%	0%	97%
QD12 LANGUAGE				
English	5%	4%	12%	17%
French	0%	0%	0%	0%

QD3A PEOPLE IN HOUSEHOLD

QD3A PEOPLE IN HOUSEHOLD

	Total Respondents	1	2	3	4	5	6
TOTAL	(2152)	17%	37%	18%	18%	7%	4%
QD1 AGE GROUP							
18-24	(132)	10%	32%	30%	14%	5%	8%
25-34	(369)	14%	32%	22%	21%	8%	4%
35-44	(566)	13%	21%	18%	29%	13%	6%
45-54	(593)	14%	28%	20%	23%	9%	5%
55-64	(345)	22%	55%	14%	7%	2%	1%
65+	(136)	32%	60%	3%	3%	1%	1%
Refused	(11)	46%	14%	19%	21%	0%	0%
QD2 REGION CMA CA							
Newfoundland	(47)	11%	46%	11%	18%	12%	3%
Nova Scotia	(192)	13%	37%	25%	20%	5%	1%
New Brunswick	(135)	16%	36%	21%	13%	12%	2%
Prince Edward Island	(18)	8%	31%	16%	25%	20%	0%
Quebec	(169)	24%	35%	16%	13%	8%	4%
Ontario	(516)	15%	35%	19%	21%	6%	4%
Manitoba	(142)	15%	42%	18%	17%	6%	2%
Saskatchewan	(74)	17%	35%	12%	25%	8%	3%
Alberta	(437)	15%	38%	19%	17%	6%	4%
British Columbia	(422)	14%	41%	18%	17%	5%	4%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	28%	33%	19%	15%	3%	2%
$25,000 To Less Than $50,000	(492)	26%	34%	19%	11%	6%	5%
$50,000 To Less Than $75,000	(488)	18%	33%	17%	18%	8%	5%
$75,000 And Over	(659)	7%	37%	18%	24%	9%	5%
Don't Know/Refused	(321)	12%	48%	16%	17%	5%	2%
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	100%	0%	0%	0%	0%	0%
2	(749)	0%	100%	0%	0%	0%	0%
3	(424)	0%	0%	100%	0%	0%	0%
4	(433)	0%	0%	0%	100%	0%	0%
5	(159)	0%	0%	0%	0%	100%	0%
6	(83)	0%	0%	0%	0%	0%	100%
Refused	(3)	0%	0%	0%	0%	0%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	1%	56%	19%	16%	5%	3%
One	(262)	0%	8%	50%	22%	14%	6%
Two	(189)	0%	0%	6%	65%	19%	10%
Three	(40)	0%	0%	0%	5%	68%	27%
Four Or More	(11)	0%	0%	0%	0%	0%	100%
Refused	(218)	99%	0%	0%	0%	0%	0%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	1%	56%	21%	16%	4%	2%
One	(275)	0%	5%	33%	36%	20%	5%
Two	(151)	0%	0%	10%	55%	25%	11%
Three	(34)	0%	0%	0%	0%	40%	60%
Four Or More	(6)	0%	0%	0%	0%	0%	100%
Refused	(218)	99%	0%	0%	0%	0%	0%
QD6 EDUCATION							
Elementary School	(26)	22%	8%	24%	13%	3%	29%
High School	(497)	17%	36%	20%	17%	7%	3%
Community College	(615)	14%	33%	20%	20%	8%	6%
University	(685)	20%	37%	15%	18%	6%	3%
Post-Graduate/Professionot Availablel	(324)	15%	44%	16%	15%	7%	3%
Don't Know/Refused	(5)	22%	41%	10%	0%	0%	0%
QD8 GENDER							
Male	(1029)	17%	38%	16%	18%	8%	3%
Female	(1123)	17%	35%	20%	18%	6%	5%
QD9 GENDERATION							
Male - 18 To 34	(223)	18%	30%	22%	17%	9%	3%
Male - 35 To 54	(529)	16%	26%	16%	25%	11%	6%
Male - 55+	(277)	16%	63%	10%	7%	3%	0%
Female - 18 To 34	(280)	9%	34%	25%	20%	5%	7%
Female - 35 To 54	(637)	11%	23%	23%	27%	11%	5%
Female - 55+	(206)	30%	50%	12%	5%	0%	2%
QD11 REGION							
Atlantic	(393)	13%	40%	20%	16%	9%	1%
Quebec	(168)	23%	34%	16%	13%	9%	5%
Ontario	(515)	15%	35%	19%	21%	6%	4%
Prairies	(652)	16%	38%	17%	19%	6%	4%
British Columbia	(424)	15%	41%	18%	16%	5%	4%
QD12 LANGUAGE							
English	(1999)	16%	37%	18%	19%	6%	4%
French	(153)	21%	35%	16%	14%	9%	5%

{sh (Continued)}

QD3A PEOPLE IN HOUSEHOLD

QD3A PEOPLE IN HOUSEHOLD

	Refused
TOTAL	0%
QD1 AGE GROUP	
18-24	0%
25-34	0%
35-44	0%
45-54	0%
55-64	0%
65+	0%
Refused	0%
QD2 REGION CMA CA	
Newfoundland	0%
Nova Scotia	0%
New Brunswick	0%
Prince Edward Island	0%
Quebec	0%
Ontario	0%
Manitoba	0%
Saskatchewan	0%
Alberta	0%
British Columbia	0%
QD3 HOUSEHOLD INCOME	
Less Than $25,000	0%
$25,000 To Less Than $50,000	0%
$50,000 To Less Than $75,000	0%
$75,000 And Over	0%
Don't Know/Refused	1%
QD3A PEOPLE IN HOUSEHOLD	
1	0%
2	0%
3	0%
4	0%
5	0%
6	0%
Refused	100%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE	
None	0%
One	0%
Two	0%
Three	0%
Four Or More	0%
Refused	1%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE	
None	0%
One	0%
Two	0%
Three	0%
Four Or More	0%
Refused	1%
QD6 EDUCATION	
Elementary School	0%
High School	0%
Community College	0%
University	0%
Post-Graduate/Professionot Availablel	0%
Don't Know/Refused	27%
QD8 GENDER	
Male	0%
Female	0%
QD9 GENDERATION	
Male - 18 To 34	0%
Male - 35 To 54	0%
Male - 55+	0%
Female - 18 To 34	0%
Female - 35 To 54	0%
Female - 55+	0%
QD11 REGION	
Atlantic	0%
Quebec	0%
Ontario	0%
Prairies	0%
British Columbia	0%
QD12 LANGUAGE	
English	0%
French	0%

QD4 HOW MANY ARE UNDER 10 YEARS OF AGE

QD4 HOW MANY ARE UNDER 10 YEARS OF AGE

	Total Respondents	None	One	Two	Three	Four Or More	Refused
TOTAL	(2077)	67%	11%	8%	1%	1%	12%
QD1 AGE GROUP							
18-24	(129)	83%	6%	3%	0%	0%	8%
25-34	(353)	50%	17%	18%	3%	2%	10%
35-44	(553)	46%	22%	17%	4%	1%	11%
45-54	(575)	75%	10%	4%	1%	1%	9%
55-64	(334)	85%	1%	0%	0%	0%	14%
65+	(124)	77%	0%	0%	0%	0%	23%
Refused	(9)	21%	22%	22%	0%	0%	35%
QD2 REGION CMA CA							
Newfoundland	(46)	73%	10%	7%	3%	0%	8%
Nova Scotia	(190)	68%	13%	7%	0%	0%	12%
New Brunswick	(129)	69%	6%	11%	3%	0%	11%
Prince Edward Island	(18)	47%	14%	18%	14%	0%	8%
Quebec	(158)	66%	10%	8%	1%	1%	14%
Ontario	(498)	68%	10%	8%	2%	1%	12%
Manitoba	(139)	65%	11%	9%	0%	1%	13%
Saskatchewan	(74)	64%	10%	10%	1%	0%	16%
Alberta	(419)	64%	14%	8%	2%	1%	11%
British Columbia	(406)	69%	12%	6%	2%	0%	10%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(172)	61%	11%	9%	1%	0%	17%
$25,000 To Less Than $50,000	(469)	61%	10%	8%	1%	1%	19%
$50,000 To Less Than $75,000	(474)	62%	13%	10%	3%	1%	12%
$75,000 And Over	(653)	74%	10%	9%	1%	1%	6%
Don't Know/Refused	(309)	76%	10%	5%	1%	0%	9%
QD3A PEOPLE IN HOUSEHOLD							
1	(226)	4%	0%	0%	0%	0%	96%
2	(749)	98%	2%	0%	0%	0%	0%
3	(424)	69%	28%	3%	0%	0%	0%
4	(433)	58%	13%	29%	0%	0%	0%
5	(159)	44%	21%	21%	14%	0%	0%
6	(83)	40%	16%	19%	9%	16%	0%
Refused	(3)	0%	0%	0%	0%	0%	100%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	100%	0%	0%	0%	0%	0%
One	(262)	0%	100%	0%	0%	0%	0%
Two	(189)	0%	0%	100%	0%	0%	0%
Three	(40)	0%	0%	0%	100%	0%	0%
Four Or More	(11)	0%	0%	0%	0%	100%	0%
Refused	(218)	0%	0%	0%	0%	0%	100%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	78%	10%	10%	2%	1%	0%
One	(275)	67%	20%	10%	2%	1%	0%
Two	(151)	78%	18%	3%	1%	0%	0%
Three	(34)	52%	20%	15%	1%	12%	0%
Four Or More	(6)	97%	0%	0%	3%	0%	0%
Refused	(218)	0%	0%	0%	0%	0%	100%
QD6 EDUCATION							
Elementary School	(25)	66%	7%	0%	0%	16%	11%
High School	(487)	67%	10%	7%	2%	0%	13%
Community College	(592)	66%	12%	11%	1%	1%	9%
University	(657)	64%	11%	8%	2%	0%	14%
Post-Graduate/Professionot Availablel	(311)	73%	9%	7%	1%	0%	10%
Don't Know/Refused	(5)	73%	0%	0%	0%	0%	27%
QD8 GENDER							
Male	(996)	67%	9%	9%	1%	1%	13%
Female	(1081)	67%	12%	8%	2%	1%	11%
QD9 GENDERATION							
Male - 18 To 34	(211)	64%	10%	9%	3%	0%	14%
Male - 35 To 54	(514)	55%	15%	14%	2%	1%	13%
Male - 55+	(271)	86%	0%	0%	0%	0%	14%
Female - 18 To 34	(273)	54%	18%	18%	2%	2%	6%
Female - 35 To 54	(619)	66%	17%	7%	2%	0%	7%
Female - 55+	(189)	80%	1%	0%	0%	0%	19%
QD11 REGION							
Atlantic	(383)	70%	10%	8%	2%	0%	9%
Quebec	(157)	66%	10%	8%	1%	2%	13%
Ontario	(497)	68%	10%	9%	2%	0%	11%
Prairies	(631)	64%	12%	9%	1%	1%	13%
British Columbia	(409)	68%	13%	6%	2%	0%	11%
QD12 LANGUAGE							
English	(1934)	67%	11%	8%	2%	0%	12%
French	(143)	66%	12%	8%	1%	2%	11%

QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE

QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE

	Total Respondents	None	One	Two	Three	Four Or More	Refused
TOTAL	(2077)	68%	11%	7%	2%	1%	12%
QD1 AGE GROUP							
18-24	(129)	73%	11%	5%	0%	2%	8%
25-34	(353)	82%	6%	2%	0%	0%	10%
35-44	(553)	52%	19%	16%	2%	1%	11%
45-54	(575)	55%	19%	11%	5%	1%	9%
55-64	(334)	80%	3%	1%	1%	0%	14%
65+	(124)	74%	3%	0%	0%	0%	23%
Refused	(9)	61%	4%	0%	0%	0%	35%
QD2 REGION CMA CA							
Newfoundland	(46)	66%	17%	4%	4%	0%	8%
Nova Scotia	(190)	71%	12%	5%	1%	0%	12%
New Brunswick	(129)	67%	16%	4%	2%	0%	11%
Prince Edward Island	(18)	86%	6%	0%	0%	0%	8%
Quebec	(158)	63%	11%	9%	2%	2%	14%
Ontario	(498)	70%	10%	6%	1%	0%	12%
Manitoba	(139)	75%	9%	3%	0%	0%	13%
Saskatchewan	(74)	62%	13%	7%	1%	0%	16%
Alberta	(419)	68%	13%	7%	1%	0%	11%
British Columbia	(406)	72%	11%	5%	2%	0%	10%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(172)	67%	11%	5%	0%	0%	17%
$25,000 To Less Than $50,000	(469)	64%	10%	5%	0%	1%	19%
$50,000 To Less Than $75,000	(474)	67%	11%	6%	3%	0%	12%
$75,000 And Over	(653)	69%	13%	9%	2%	1%	6%
Don't Know/Refused	(309)	77%	8%	5%	1%	0%	9%
QD3A PEOPLE IN HOUSEHOLD							
1	(226)	4%	0%	0%	0%	0%	96%
2	(749)	99%	1%	0%	0%	0%	0%
3	(424)	77%	20%	3%	0%	0%	0%
4	(433)	59%	21%	20%	0%	0%	0%
5	(159)	38%	31%	23%	9%	0%	0%
6	(83)	33%	14%	17%	22%	14%	0%
Refused	(3)	0%	0%	0%	0%	0%	100%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	79%	11%	8%	1%	1%	0%
One	(262)	66%	20%	11%	3%	0%	0%
Two	(189)	81%	14%	3%	3%	0%	0%
Three	(40)	78%	16%	4%	1%	1%	0%
Four Or More	(11)	54%	15%	4%	27%	0%	0%
Refused	(218)	0%	0%	0%	0%	0%	100%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	100%	0%	0%	0%	0%	0%
One	(275)	0%	100%	0%	0%	0%	0%
Two	(151)	0%	0%	100%	0%	0%	0%
Three	(34)	0%	0%	0%	100%	0%	0%
Four Or More	(6)	0%	0%	0%	0%	100%	0%
Refused	(218)	0%	0%	0%	0%	0%	100%
QD6 EDUCATION							
Elementary School	(25)	49%	21%	3%	16%	0%	11%
High School	(487)	67%	12%	6%	1%	1%	13%
Community College	(592)	69%	11%	8%	1%	1%	9%
University	(657)	66%	11%	7%	1%	0%	14%
Post-Graduate/Professionot Availablel	(311)	74%	8%	5%	2%	0%	10%
Don't Know/Refused	(5)	63%	10%	0%	0%	0%	27%
QD8 GENDER							
Male	(996)	68%	11%	5%	2%	0%	13%
Female	(1081)	69%	11%	8%	1%	1%	11%
QD9 GENDERATION							
Male - 18 To 34	(211)	74%	9%	2%	0%	1%	14%
Male - 35 To 54	(514)	56%	18%	9%	5%	0%	13%
Male - 55+	(271)	80%	5%	1%	0%	0%	14%
Female - 18 To 34	(273)	84%	7%	3%	0%	0%	6%
Female - 35 To 54	(619)	52%	21%	18%	1%	1%	7%
Female - 55+	(189)	77%	1%	1%	1%	1%	19%
QD11 REGION							
Atlantic	(383)	71%	14%	4%	2%	0%	9%
Quebec	(157)	62%	11%	9%	2%	2%	13%
Ontario	(497)	70%	10%	6%	1%	0%	11%
Prairies	(631)	68%	12%	6%	1%	0%	13%
British Columbia	(409)	72%	10%	5%	2%	0%	11%
QD12 LANGUAGE							
English	(1934)	70%	11%	6%	2%	0%	12%
French	(143)	62%	13%	10%	1%	2%	11%

QD6 EDUCATION

QD6 EDUCATION

	Total Respondents	Elementary School	High School	Community College	University	Post-Graduate/ Professionot Availablel	Don't Know/Refused
TOTAL	(2152)	1%	24%	27%	32%	16%	0%
QD1 AGE GROUP							
18-24	(132)	2%	49%	27%	17%	5%	0%
25-34	(369)	0%	15%	31%	41%	12%	0%
35-44	(566)	1%	18%	33%	32%	16%	0%
45-54	(593)	1%	23%	30%	30%	14%	1%
55-64	(345)	1%	27%	22%	31%	18%	0%
65+	(136)	0%	27%	12%	28%	33%	0%
Refused	(11)	0%	25%	16%	32%	26%	0%
QD2 REGION CMA CA							
Newfoundland	(47)	1%	10%	46%	18%	25%	0%
Nova Scotia	(192)	1%	23%	27%	35%	14%	0%
New Brunswick	(135)	2%	21%	27%	41%	9%	0%
Prince Edward Island	(18)	12%	2%	59%	20%	8%	0%
Quebec	(169)	1%	24%	30%	33%	13%	0%
Ontario	(516)	1%	23%	24%	32%	19%	0%
Manitoba	(142)	2%	30%	24%	33%	11%	0%
Saskatchewan	(74)	0%	27%	22%	42%	8%	0%
Alberta	(437)	2%	23%	28%	32%	14%	0%
British Columbia	(422)	0%	26%	29%	27%	17%	0%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	2%	33%	28%	23%	12%	1%
$25,000 To Less Than $50,000	(492)	1%	28%	35%	28%	9%	0%
$50,000 To Less Than $75,000	(488)	1%	22%	31%	36%	10%	0%
$75,000 And Over	(659)	0%	15%	19%	36%	29%	0%
Don't Know/Refused	(321)	1%	32%	24%	29%	14%	0%
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	1%	24%	22%	39%	14%	0%
2	(749)	0%	24%	25%	32%	19%	0%
3	(424)	1%	27%	30%	27%	14%	0%
4	(433)	1%	22%	30%	33%	13%	0%
5	(159)	1%	23%	34%	26%	17%	0%
6	(83)	7%	20%	38%	24%	10%	0%
Refused	(3)	0%	0%	0%	54%	0%	46%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	1%	24%	27%	30%	17%	0%
One	(262)	1%	23%	30%	32%	14%	0%
Two	(189)	0%	20%	37%	30%	13%	0%
Three	(40)	0%	30%	19%	38%	13%	0%
Four Or More	(11)	23%	4%	45%	19%	8%	0%
Refused	(218)	1%	27%	20%	38%	13%	1%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	1%	24%	28%	30%	17%	0%
One	(275)	2%	27%	28%	31%	11%	0%
Two	(151)	0%	20%	35%	31%	13%	0%
Three	(34)	10%	8%	26%	30%	25%	0%
Four Or More	(6)	0%	28%	59%	10%	3%	0%
Refused	(218)	1%	27%	20%	38%	13%	1%
QD6 EDUCATION							
Elementary School	(26)	100%	0%	0%	0%	0%	0%
High School	(497)	0%	100%	0%	0%	0%	0%
Community College	(615)	0%	0%	100%	0%	0%	0%
University	(685)	0%	0%	0%	100%	0%	0%
Post-Graduate/Professionot Availablel	(324)	0%	0%	0%	0%	100%	0%
Don't Know/Refused	(5)	0%	0%	0%	0%	0%	100%
QD8 GENDER							
Male	(1029)	1%	19%	26%	35%	18%	0%
Female	(1123)	1%	28%	29%	29%	13%	0%
QD9 GENDERATION							
Male - 18 To 34	(223)	1%	24%	27%	36%	12%	0%
Male - 35 To 54	(529)	2%	16%	28%	36%	17%	1%
Male - 55+	(277)	0%	20%	21%	32%	27%	0%
Female - 18 To 34	(280)	0%	25%	33%	33%	8%	0%
Female - 35 To 54	(637)	1%	25%	35%	26%	13%	0%
Female - 55+	(206)	2%	33%	19%	29%	17%	0%
QD11 REGION							
Atlantic	(393)	2%	18%	32%	35%	14%	0%
Quebec	(168)	1%	24%	30%	32%	13%	0%
Ontario	(515)	1%	24%	24%	32%	19%	0%
Prairies	(652)	1%	26%	26%	34%	13%	0%
British Columbia	(424)	0%	25%	28%	28%	17%	0%
QD12 LANGUAGE							
English	(1999)	1%	24%	26%	32%	16%	0%
French	(153)	1%	22%	31%	33%	14%	0%

QD3 HOUSEHOLD INCOME

QD3 HOUSEHOLD INCOME

	Total Respondents	Less Than $25,000	$25,000 To Less Than $50,000	$50,000 To Less Than $75,000	$75,000 And Over	Don't Know/Refused
TOTAL	(2152)	10%	24%	24%	29%	14%
QD1 AGE GROUP						
18-24	(132)	31%	20%	16%	19%	14%
25-34	(369)	16%	27%	24%	23%	10%
35-44	(566)	8%	26%	25%	33%	9%
45-54	(593)	7%	14%	26%	36%	17%
55-64	(345)	4%	30%	24%	27%	16%
65+	(136)	5%	27%	24%	29%	15%
Refused	(11)	0%	3%	0%	0%	97%
QD2 REGION CMA CA						
Newfoundland	(47)	13%	33%	15%	22%	16%
Nova Scotia	(192)	11%	32%	21%	23%	14%
New Brunswick	(135)	11%	21%	23%	24%	21%
Prince Edward Island	(18)	0%	39%	24%	27%	10%
Quebec	(169)	13%	32%	28%	16%	10%
Ontario	(516)	8%	18%	23%	37%	14%
Manitoba	(142)	9%	20%	26%	28%	17%
Saskatchewan	(74)	11%	25%	19%	35%	8%
Alberta	(437)	7%	23%	21%	30%	19%
British Columbia	(422)	7%	26%	23%	29%	14%
QD3 HOUSEHOLD INCOME						
Less Than $25,000	(192)	100%	0%	0%	0%	0%
$25,000 To Less Than $50,000	(492)	0%	100%	0%	0%	0%
$50,000 To Less Than $75,000	(488)	0%	0%	100%	0%	0%
$75,000 And Over	(659)	0%	0%	0%	100%	0%
Don't Know/Refused	(321)	0%	0%	0%	0%	100%
QD3A PEOPLE IN HOUSEHOLD						
1	(301)	16%	37%	26%	12%	9%
2	(749)	9%	22%	22%	29%	18%
3	(424)	11%	26%	23%	29%	12%
4	(433)	8%	15%	25%	39%	13%
5	(159)	4%	22%	27%	38%	10%
6	(83)	5%	27%	29%	33%	6%
Refused	(3)	0%	0%	37%	0%	63%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE						
None	(1357)	8%	22%	21%	33%	16%
One	(262)	9%	22%	28%	28%	12%
Two	(189)	10%	22%	28%	32%	8%
Three	(40)	6%	16%	42%	25%	10%
Four Or More	(11)	0%	37%	37%	27%	0%
Refused	(218)	13%	39%	23%	14%	11%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE						
None	(1393)	9%	23%	23%	30%	16%
One	(275)	9%	21%	23%	36%	11%
Two	(151)	6%	19%	22%	42%	10%
Three	(34)	0%	5%	50%	39%	6%
Four Or More	(6)	0%	39%	20%	41%	0%
Refused	(218)	13%	39%	23%	14%	11%
QD6 EDUCATION						
Elementary School	(26)	23%	36%	21%	8%	12%
High School	(497)	14%	28%	22%	18%	18%
Community College	(615)	10%	31%	27%	20%	12%
University	(685)	7%	21%	27%	33%	12%
Post-Graduate/Professionot Availablel	(324)	8%	14%	15%	52%	12%
Don't Know/Refused	(5)	22%	0%	23%	27%	27%
QD8 GENDER						
Male	(1029)	8%	24%	24%	33%	11%
Female	(1123)	11%	25%	24%	24%	16%
QD9 GENDERATION						
Male - 18 To 34	(223)	19%	26%	25%	19%	11%
Male - 35 To 54	(529)	5%	20%	25%	38%	12%
Male - 55+	(277)	3%	26%	21%	39%	10%
Female - 18 To 34	(280)	21%	24%	19%	25%	11%
Female - 35 To 54	(637)	9%	20%	25%	30%	15%
Female - 55+	(206)	5%	31%	26%	18%	20%
QD11 REGION						
Atlantic	(393)	10%	31%	20%	23%	15%
Quebec	(168)	13%	32%	28%	17%	10%
Ontario	(515)	8%	18%	23%	37%	14%
Prairies	(652)	8%	23%	22%	30%	16%
British Columbia	(424)	7%	26%	23%	29%	15%
QD12 LANGUAGE						
English	(1999)	8%	23%	22%	32%	15%
French	(153)	14%	29%	29%	17%	10%

QD8 GENDER

QD8 GENDER

	Total Respondents	Male	Female
TOTAL	(2152)	48%	52%
QD1 AGE GROUP			
18-24	(132)	46%	54%
25-34	(369)	51%	49%
35-44	(566)	51%	49%
45-54	(593)	49%	51%
55-64	(345)	37%	63%
65+	(136)	62%	38%
Refused	(11)	52%	48%
QD2 REGION CMA CA			
Newfoundland	(47)	46%	54%
Nova Scotia	(192)	50%	50%
New Brunswick	(135)	48%	52%
Prince Edward Island	(18)	41%	59%
Quebec	(169)	46%	54%
Ontario	(516)	48%	52%
Manitoba	(142)	49%	51%
Saskatchewan	(74)	50%	50%
Alberta	(437)	50%	50%
British Columbia	(422)	48%	52%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	41%	59%
$25,000 To Less Than $50,000	(492)	46%	54%
$50,000 To Less Than $75,000	(488)	47%	53%
$75,000 And Over	(659)	55%	45%
Don't Know/Refused	(321)	38%	62%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	47%	53%
2	(749)	49%	51%
3	(424)	42%	58%
4	(433)	47%	53%
5	(159)	57%	43%
6	(83)	40%	60%
Refused	(3)	63%	37%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	48%	52%
One	(262)	42%	58%
Two	(189)	51%	49%
Three	(40)	48%	52%
Four Or More	(11)	38%	62%
Refused	(218)	54%	46%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	48%	52%
One	(275)	50%	50%
Two	(151)	35%	65%
Three	(34)	68%	32%
Four Or More	(6)	32%	68%
Refused	(218)	54%	46%
QD6 EDUCATION			
Elementary School	(26)	58%	42%
High School	(497)	39%	61%
Community College	(615)	45%	55%
University	(685)	52%	48%
Post-Graduate/Professionot Availablel	(324)	55%	45%
Don't Know/Refused	(5)	68%	32%
QD8 GENDER			
Male	(1029)	100%	0%
Female	(1123)	0%	100%
QD9 GENDERATION			
Male - 18 To 34	(223)	100%	0%
Male - 35 To 54	(529)	100%	0%
Male - 55+	(277)	100%	0%
Female - 18 To 34	(280)	0%	100%
Female - 35 To 54	(637)	0%	100%
Female - 55+	(206)	0%	100%
QD11 REGION			
Atlantic	(393)	50%	50%
Quebec	(168)	45%	55%
Ontario	(515)	48%	52%
Prairies	(652)	49%	51%
British Columbia	(424)	48%	52%
QD12 LANGUAGE			
English	(1999)	49%	51%
French	(153)	43%	57%

QD9 GENDERATION

QD9 GENDERATION

	Total Respondents	Male - 18 To 34	Male - 35 To 54	Male - 55+	Female - 18 To 34	Female - 35 To 54	Female - 55+
TOTAL	(2152)	13%	20%	14%	13%	21%	18%
QD1 AGE GROUP							
18-24	(132)	46%	0%	0%	54%	0%	0%
25-34	(369)	51%	0%	0%	49%	0%	0%
35-44	(566)	0%	51%	0%	0%	49%	0%
45-54	(593)	0%	49%	0%	0%	51%	0%
55-64	(345)	0%	0%	37%	0%	0%	63%
65+	(136)	0%	0%	62%	0%	0%	38%
Refused	(11)	18%	23%	11%	6%	31%	11%
QD2 REGION CMA CA							
Newfoundland	(47)	11%	21%	14%	17%	21%	17%
Nova Scotia	(192)	14%	18%	17%	12%	22%	16%
New Brunswick	(135)	15%	20%	13%	12%	21%	18%
Prince Edward Island	(18)	0%	29%	12%	12%	47%	0%
Quebec	(169)	13%	20%	13%	13%	19%	22%
Ontario	(516)	13%	21%	14%	14%	21%	18%
Manitoba	(142)	14%	19%	16%	13%	22%	16%
Saskatchewan	(74)	13%	18%	19%	12%	20%	19%
Alberta	(437)	16%	23%	12%	14%	22%	15%
British Columbia	(422)	14%	19%	15%	14%	20%	18%
QD3 HOUSEHOLD INCOME							
Less Than $25,000	(192)	26%	11%	5%	29%	20%	9%
$25,000 To Less Than $50,000	(492)	14%	17%	15%	13%	17%	24%
$50,000 To Less Than $75,000	(488)	14%	21%	12%	10%	22%	20%
$75,000 And Over	(659)	9%	27%	19%	12%	21%	12%
Don't Know/Refused	(321)	10%	18%	10%	11%	23%	27%
QD3A PEOPLE IN HOUSEHOLD							
1	(301)	14%	20%	13%	7%	13%	33%
2	(749)	11%	15%	24%	13%	13%	25%
3	(424)	17%	18%	8%	19%	27%	12%
4	(433)	13%	29%	6%	15%	32%	5%
5	(159)	18%	33%	7%	10%	33%	0%
6	(83)	11%	30%	0%	22%	27%	10%
Refused	(3)	0%	63%	0%	0%	37%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE							
None	(1357)	13%	17%	18%	11%	21%	20%
One	(262)	12%	30%	0%	23%	34%	2%
Two	(189)	15%	36%	0%	30%	19%	0%
Three	(40)	24%	24%	0%	17%	35%	0%
Four Or More	(11)	5%	34%	0%	46%	15%	0%
Refused	(218)	15%	22%	17%	7%	12%	27%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE							
None	(1393)	14%	17%	17%	17%	16%	19%
One	(275)	10%	33%	6%	9%	40%	2%
Two	(151)	4%	28%	3%	6%	56%	2%
Three	(34)	0%	66%	2%	2%	20%	11%
Four Or More	(6)	28%	3%	0%	0%	49%	20%
Refused	(218)	15%	22%	17%	7%	12%	27%
QD6 EDUCATION							
Elementary School	(26)	11%	43%	4%	3%	12%	28%
High School	(497)	14%	14%	11%	14%	21%	26%
Community College	(615)	13%	21%	11%	16%	26%	13%
University	(685)	15%	23%	14%	14%	17%	17%
Post-Graduate/Professionot Availablel	(324)	10%	22%	24%	7%	17%	20%
Don't Know/Refused	(5)	0%	55%	14%	0%	32%	0%
QD8 GENDER							
Male	(1029)	28%	43%	29%	0%	0%	0%
Female	(1123)	0%	0%	0%	26%	39%	35%
QD9 GENDERATION							
Male - 18 To 34	(223)	100%	0%	0%	0%	0%	0%
Male - 35 To 54	(529)	0%	100%	0%	0%	0%	0%
Male - 55+	(277)	0%	0%	100%	0%	0%	0%
Female - 18 To 34	(280)	0%	0%	0%	100%	0%	0%
Female - 35 To 54	(637)	0%	0%	0%	0%	100%	0%
Female - 55+	(206)	0%	0%	0%	0%	0%	100%
QD11 REGION							
Atlantic	(393)	13%	19%	18%	13%	22%	16%
Quebec	(168)	13%	20%	12%	13%	20%	22%
Ontario	(515)	13%	21%	14%	14%	21%	18%
Prairies	(652)	14%	20%	14%	13%	21%	16%
British Columbia	(424)	13%	20%	15%	14%	20%	18%
QD12 LANGUAGE							
English	(1999)	13%	20%	15%	13%	20%	18%
French	(153)	13%	22%	8%	14%	22%	21%

QD11 REGION

QD11 REGION

	Total Respondents	Atlantic	Quebec	Ontario	Prairies	British Columbia
TOTAL	(2152)	8%	25%	37%	16%	13%
QD1 AGE GROUP						
18-24	(132)	6%	30%	37%	18%	9%
25-34	(369)	8%	23%	37%	16%	16%
35-44	(566)	7%	26%	38%	17%	12%
45-54	(593)	8%	24%	38%	17%	13%
55-64	(345)	8%	31%	33%	15%	13%
65+	(136)	7%	13%	47%	18%	15%
Refused	(11)	3%	0%	43%	17%	37%
QD2 REGION CMA CA						
Newfoundland	(47)	97%	0%	0%	0%	3%
Nova Scotia	(192)	100%	0%	0%	0%	0%
New Brunswick	(135)	100%	0%	0%	0%	0%
Prince Edward Island	(18)	92%	0%	0%	8%	0%
Quebec	(169)	1%	99%	0%	0%	0%
Ontario	(516)	0%	0%	99%	0%	1%
Manitoba	(142)	0%	0%	0%	100%	0%
Saskatchewan	(74)	0%	0%	4%	96%	0%
Alberta	(437)	0%	0%	0%	99%	1%
British Columbia	(422)	0%	0%	0%	1%	98%
QD3 HOUSEHOLD INCOME						
Less Than $25,000	(192)	8%	35%	33%	14%	10%
$25,000 To Less Than $50,000	(492)	10%	33%	27%	16%	15%
$50,000 To Less Than $75,000	(488)	6%	30%	36%	15%	13%
$75,000 And Over	(659)	6%	15%	48%	17%	14%
Don't Know/Refused	(321)	9%	18%	39%	19%	14%
QD3A PEOPLE IN HOUSEHOLD						
1	(301)	6%	35%	32%	16%	12%
2	(749)	9%	24%	36%	17%	15%
3	(424)	9%	22%	40%	16%	14%
4	(433)	7%	19%	44%	18%	12%
5	(159)	11%	32%	32%	15%	11%
6	(83)	3%	31%	36%	15%	15%
Refused	(3)	0%	0%	83%	0%	17%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE						
None	(1357)	8%	23%	38%	16%	14%
One	(262)	7%	23%	35%	19%	16%
Two	(189)	8%	24%	40%	17%	11%
Three	(40)	13%	11%	43%	14%	19%
Four Or More	(11)	0%	62%	19%	16%	4%
Refused	(218)	6%	27%	36%	18%	12%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE						
None	(1393)	8%	22%	39%	17%	14%
One	(275)	10%	25%	35%	18%	12%
Two	(151)	5%	33%	37%	15%	10%
Three	(34)	9%	30%	32%	11%	18%
Four Or More	(6)	0%	67%	29%	3%	0%
Refused	(218)	6%	27%	36%	18%	12%
QD6 EDUCATION						
Elementary School	(26)	14%	29%	29%	23%	5%
High School	(497)	6%	26%	37%	18%	14%
Community College	(615)	9%	28%	33%	16%	14%
University	(685)	9%	25%	37%	18%	12%
Post-Graduate/Professionot Availablel	(324)	7%	20%	45%	13%	15%
Don't Know/Refused	(5)	0%	0%	77%	0%	23%
QD8 GENDER						
Male	(1029)	8%	24%	37%	17%	14%
Female	(1123)	7%	26%	37%	16%	13%
QD9 GENDERATION						
Male - 18 To 34	(223)	8%	24%	37%	18%	13%
Male - 35 To 54	(529)	7%	25%	38%	16%	13%
Male - 55+	(277)	10%	22%	37%	17%	14%
Female - 18 To 34	(280)	7%	24%	38%	16%	14%
Female - 35 To 54	(637)	8%	24%	38%	17%	13%
Female - 55+	(206)	7%	30%	36%	14%	13%
QD11 REGION						
Atlantic	(393)	100%	0%	0%	0%	0%
Quebec	(168)	0%	100%	0%	0%	0%
Ontario	(515)	0%	0%	100%	0%	0%
Prairies	(652)	0%	0%	0%	100%	0%
British Columbia	(424)	0%	0%	0%	0%	100%
QD12 LANGUAGE						
English	(1999)	10%	4%	48%	21%	17%
French	(153)	0%	100%	0%	0%	0%

QD12 LANGUAGE

QD12 LANGUAGE

	Total Respondents	English	French
TOTAL	(2152)	78%	22%
QD1 AGE GROUP			
18-24	(132)	72%	28%
25-34	(369)	79%	21%
35-44	(566)	76%	24%
45-54	(593)	77%	23%
55-64	(345)	76%	24%
65+	(136)	93%	7%
Refused	(11)	100%	0%
QD2 REGION CMA CA			
Newfoundland	(47)	100%	0%
Nova Scotia	(192)	100%	0%
New Brunswick	(135)	100%	0%
Prince Edward Island	(18)	100%	0%
Quebec	(169)	14%	86%
Ontario	(516)	100%	0%
Manitoba	(142)	100%	0%
Saskatchewan	(74)	100%	0%
Alberta	(437)	100%	0%
British Columbia	(422)	100%	0%
QD3 HOUSEHOLD INCOME			
Less Than $25,000	(192)	67%	33%
$25,000 To Less Than $50,000	(492)	74%	26%
$50,000 To Less Than $75,000	(488)	73%	27%
$75,000 And Over	(659)	87%	13%
Don't Know/Refused	(321)	84%	16%
QD3A PEOPLE IN HOUSEHOLD			
1	(301)	73%	27%
2	(749)	79%	21%
3	(424)	81%	19%
4	(433)	82%	18%
5	(159)	72%	28%
6	(83)	73%	27%
Refused	(3)	100%	0%
QD4 HOW MANY ARE UNDER 10 YEARS OF AGE			
None	(1357)	79%	21%
One	(262)	77%	23%
Two	(189)	79%	21%
Three	(40)	89%	11%
Four Or More	(11)	38%	62%
Refused	(218)	80%	20%
QD5 HOW MANY BETWEEN 10-17 YEARS OF AGE			
None	(1393)	81%	19%
One	(275)	75%	25%
Two	(151)	67%	33%
Three	(34)	80%	20%
Four Or More	(6)	33%	67%
Refused	(218)	80%	20%
QD6 EDUCATION			
Elementary School	(26)	71%	29%
High School	(497)	80%	20%
Community College	(615)	75%	25%
University	(685)	77%	23%
Post-Graduate/Professionot Availablel	(324)	81%	19%
Don't Know/Refused	(5)	100%	0%
QD8 GENDER			
Male	(1029)	80%	20%
Female	(1123)	76%	24%
QD9 GENDERATION			
Male - 18 To 34	(223)	78%	22%
Male - 35 To 54	(529)	76%	24%
Male - 55+	(277)	87%	13%
Female - 18 To 34	(280)	77%	23%
Female - 35 To 54	(637)	77%	23%
Female - 55+	(206)	75%	25%
QD11 REGION			
Atlantic	(393)	100%	0%
Quebec	(168)	13%	87%
Ontario	(515)	100%	0%
Prairies	(652)	100%	0%
British Columbia	(424)	100%	0%
QD12 LANGUAGE			
English	(1999)	100%	0%
French	(153)	0%	100%