ELECTRONIC PRIVACY INFORMATION CENTER

Before the
Federal Trade Commission
Washington, D.C. 20580

In the Matter of	**)**	
	)	
Public Workshop--Monitoring Software	**)**	**FTC File No. P044509**
on Your PC: Spyware, Adware, and	**)**	
Other Software	**)**	

To: The Commission

PRELIMINARY COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER
April 19, 2004

We applaud the Federal Trade Commission for holding a public workshop to address "Monitoring Software on Your PC: Spyware, Adware, and Other Software."[1] We have posed answers to selected questions from the Federal Register notice below. In our comments below, we argue that spyware is difficult to define; that many so called "legitimate" models of information collection could be considered spyware, and that the Commission should not focus on peer-to-peer networks as a primary source for invasive information collection online. We further comment that many incipient Digital Rights Management (DRM) systems strongly resemble spyware, and should be closely monitored by the Commission.

We wish to first comment that consumers would be better served with a general privacy law rather than a new, sectoral regulation that only targets data collection in the narrow category of "spyware." A generally-applicable privacy statute based on a full set of fair information practices would limit collect of information across the board, providing legal protections against spyware and so called "legitimate" information transfers. Narrowly addressing this problem will result in not addressing current and future invasive technologies that fall outside the definition of "spyware." Narrowly addressing spyware also serves to legitimatize other invasive collections of personal information.

[1] Public Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software; Notice, 69 Fed. Reg. 8537 (Feb. 24, 2004), available at http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/04-3979.htm

A. Defining and Understanding Spyware.

i. What types of software (particularly downloaded software) should be considered "spyware"?

It is difficult to define spyware in a manner that is not either over-inclusive or under-inclusive. Below, some indicia of invasiveness are listed that commonly appear in spyware and other privacy-unfriendly programs:

- Commercial activity or use of computing power that is unrelated to the user's intended use of the software
  - Port listening (monitoring of basic internet traffic) other than that which is fundamentally required for the software's purpose.
  - Use of computer resources (*e.g.* distributed computing).
  - The program causes the computer to contact and download content or additional software for commercial purposes.
  - The program transmits identifying data to third party servers.
- Poor notice to users
  - Combined EULAs, such that agreeing to one program agrees to bundled spyware.
  - When updates are installed, particularly ones that change potentially objectionable behavior, there is no warning message or EULA.
  - Installs functionality or displays advertising without the consent of the user.
  - Uses opt-out mechanisms or other methods with inadequate user interaction for subscription to services such as e-mail lists.
- Incomplete removal or "respawning," the reestablishment of the program
  - Removing main program does not delete spyware functions.
  - If spyware or main software is deleted, spyware re-installs itself or re-downloads its main components through a "trickler."
  - Software that quietly restarts itself or runs at boot through placing keys in the computer's registry.
- Misdirection
  - The EULA doesn't list all of the third party servers that will be contacted.
  - When resources are clicked, the user is directed to the website of some party other than the one they committed to contact.
- Security threats
  - Personal information submitted to or through the spyware is sent or stored in the clear (without encryption).
  - The program scans stored files unrelated to the function of the program (e.g., scans all of the files on user's hard drive).
  - Software that monitors keystrokes or other user interaction for surveillance or stalking purposes.
- Poor privacy Practices
  - Software is serialized – every instance of the software contains a unique identifier.
  - Employs persistent cookies.

- Frequently communicates to the home server for "updates" that are for advertising or identifying purposes or otherwise unrelated to the core functionality of the software.

These indicia of invasiveness are not limited to shadowy spyware programs. More "legitimate" companies have also employed many of these techniques to track individuals. For instance, in 1999, Internet security expert Richard M. Smith discovered that Real Network's Real Jukebox employed serialization and extensive tracking of users:

> …RealJukeBox software is sending off information to RealNetworks about what music CDs I listen to, along with a unique player ID number that identifies who I am. I also found that the RealJukeBox sends back to RealNetworks, on a daily basis, information on how I am using the product. It reports things like how many songs I have recorded on my hard drive, the type of portable MP3 player I own, and my music preferences.
>
> This monitoring system, built into the RealJukeBox software, has the potential for being used as a powerful profiling system to help market new CDs and related products at the expense of personal privacy…
>
> The RealJukeBox is now the default music CD player on my Windows system. I noticed that each time I play a music CD in my computer CD-ROM drive, that RealJukeBox player shows the name of the CD, the artist, and a list of all songs on the CD. This is a pretty handy feature if one wants to only listen to or record one or two tracks on a CD. All of this information about the music CD is obtained from a Web server at RealNetworks. This information is downloaded in parallel when a CD starts playing.
>
> I decided to put a packet sniffer on the RealJukeBox player to see exactly what information is being transmitted from my computer to the Real Networks servers. Mucmh [sic] to my dismay, I found that in the HTTP GET request for the CD information, the player is including a unique GUID serial number for my copy of the software.[2]

A similar problem arose with Windows Media Player for Windows XP.[3] Again, Richard M. Smith found significant spyware-like properties in this software:

> I found a number of serious privacy problems with Microsoft's Windows Media Player (WMP) for Windows XP. A number of design choices were made in WMP which allow Microsoft to individually track what DVD movies consumers are watching on their Windows PC. These problems which introduced in version 8 of WMP which ships preinstalled on all Windows XP systems.

---

[2] Richard M. Smith, *The RealJukeBox monitoring system*, Oct. 31, 1999, available at http://www.computerbytesman.com/privacy/realjb.htm.

[3] Richard M. Smith, *Serious privacy problems in Windows Media Player for Windows XP*, Feb. 20, 2002, available at http://computerbytesman.com/privacy/wmp8dvd.htm.

In particular, the privacy problems with WMP version 8 are:

* Each time a new DVD movie is played on a computer, the WMP software contacts a Microsoft Web server to get title and chapter information for the DVD. When this contact is made, the Microsoft Web server is given an electronic fingerprint which identifies the DVD movie being watched and a cookie which uniquely identifies a particular WMP player. With this two pieces of information Microsoft can track what DVD movies are being watched on a particular computer.

* The WMP software also builds a small database on the computer hard drive of all DVD movies that have been watched on the computer.

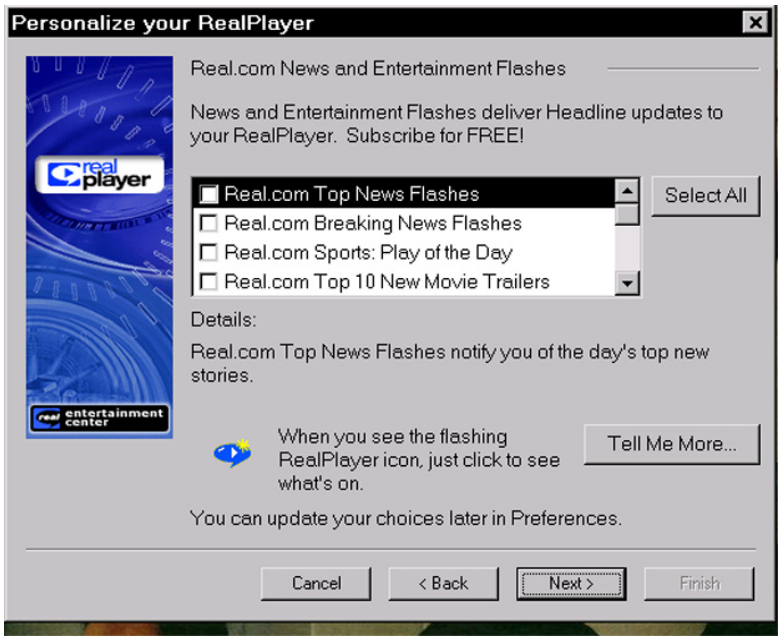
* As of Feb. 14, 2002, the Microsoft privacy policy for WMP version 8 does not disclose that the fact that WMP "phones home" to get DVD title information, what kind of tracking Microsoft does of which movies consumers are watching, and how cookies are used by the WMP software and the Microsoft servers.

* There does not appear to be any option in WMP to stop it from phoning home when a DVD movie is viewed. In addition, there does not appear any easy method of clearing out the DVD movie database on the local hard drive.

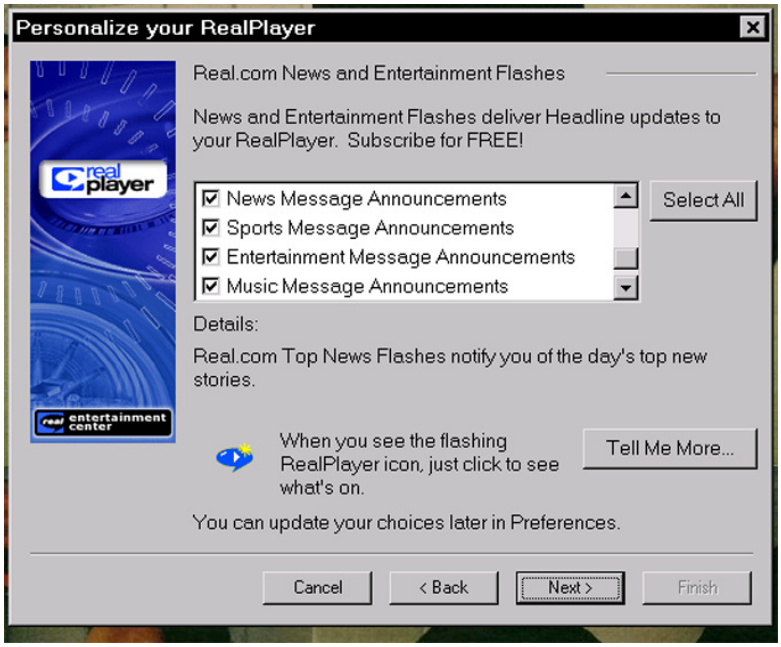
Because Windows Media Player is serialized, it poses serious risks for tracking of Internet browsing: "There is a significant privacy problem with Internet Explorer because of a design flaw in the Windows Media Player (WMP). Using simple Javascript code on a Web page, a Web site can grab the unique ID number of the Windows Media Player belonging to a Web site visitor. This ID number can then be used just like a cookie by Web sites to track a user's travels around the Web."[4]

[4] Richard M. Smith, *Internet Explorer SuperCookies bypass P3P and cookie controls*, Jan. 16, 2002, available at http://www.computerbytesman.com/privacy/supercookie.htm.

Many legitimate programs continue to collect personally-identifiable information unnecessarily, or attempt to gain consent from the user in a deceptive fashion. In previous versions of Realnetworks Real Player, the company attempted to gain consent from users to receive real.com messages by placing opt-out options below the users' view. In the figure below, users are asked to "personalize" the software by subscribing to headlines. The four choices in view to the user are unchecked.



However, if the user scrolls the option window down, she will find that Realnetworks has left several headlines selected. These headlines appear to cover a broader scope of "headlines" than the displayed (and unchecked) ones listed above.



To this day, Realnetworks' current player software, which is in version 10, requires users to give their e-mail address and zip code at installation. It continues to rely upon an opt-out model for subscriptions to its information services. None of this information is relevant to the actual use of the player software, which is required to view broadcasts of many public government events, such as Congressional hearings, C-SPAN, and the like.

Because software propagated by so called "legitimate" companies have employed indicia of spyware, the Federal Trade Commission should focus on voluntariness of information collection rather than the label "spyware." Quality of consent is the key issue underlying collection of information. With spyware, the quality of consent or voluntariness is particularly low, but sometimes it is also low with other so called "legitimate" tools of automated data collection, including cookies, and the software applications listed above.

The Commission should consider some Digital Rights Management ("DRM") systems as forms of spyware.[5] DRMs restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving.

Some existing DRM systems implicate privacy because they allow copyright owners to monitor private consumption of content. In an attempt to secure content, many DRM systems require the user to identify and authenticate a right of access to the protected media. In the case of Microsoft's eBook Reader, this means that the media software and users' choices in electronic books are digitally linked not only to the user's computer, but also to the company's identity management system, Microsoft Passport.[6] This arrangement allows tracking of both the individual and the individuals' computer.

A recent lawsuit illustrates how DRM implementations can be privacy invasive. In February 2002, Sunncomm, Inc., a DRM systems developer, and Music City Records settled a lawsuit by a California woman who objected to their practice of tracking and disclosing personal information—including music consumption patterns—to third-parties with no opt-out scheme. In the case, the plaintiff's attorney, Ira Rothken filed suit under a broad California consumer protection statute, arguing that SunnComm: "never disclose[d] on the shrink-wrap of the CD(s) that consumers cannot listen to music on their computers anonymously. If left unchecked, this will be the start of an era where consumers will be coerced to give up their privacy to listen to music on their computers."[7] The settlement agreement required the companies to provide notice

---

[5] *See generally* Chris Jay Hoofnagle, *Digital Rights Management: Many Technical Controls on Digital Content Distribution Can Create A Surveillance Society*, Colum. Sci. & Tech. L. Rev. (forthcoming 2004); Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management in Cyberspace*, 28 Conn. L. Rev. 981 (1996).

[6] This service is now called ".Net Passport." Russel Kay, *Copy Protection: Just Say No*, Computerworld, (Sept. 4, 2000); Chris Jay Hoofnagle, *Overview of Consumer Privacy 2002*, 701 Practicing Law Institute 1339 (2002), at http://www.epic.org/epic/staff/hoofnagle/plidraft2002.pdf; Chris Jay Hoofnagle, *Digital Rights Management and Privacy*, Presentation to the Santa Clara University Law School Symposium on Information Insecurity, Feb. 8, 2002, at http://www.epic.org/epic/staff/hoofnagle/drm.ppt; Megan E. Gray & Will Thomas DeVries, *The Legal Fallout From Digital Rights Management Technology*, 20 Comp. & Internet Lawyer 20 (April 2003).

[7] DeLise v. Fahrenheit, No. CV-014297 (Cal. Sup. Ct. Sept. 6, 2001)(Pl. Comp. at ¶ 1), available at http://www.techfirm.com/mccomp.pdf.

to consumers of their information collection practices and to refrain from requiring consumers to disclose their personal information as a condition of downloading, playing, or listening to a CD.[8]

While this settlement agreement is important, not all Americans can avail themselves of California's consumer protection laws. Given adequate notice to consumers, it is likely that other states and the Commission will not object to Sunncomm-style DRMs, and assume that the user consciously and freely accepted the invasion of their privacy when buying the product. Users of these new systems will be taken from a culture where there is freedom to enjoy media anonymously to one where access will be conditioned upon revealing one's identity. And once the individual has given up their freedom of anonymity, media companies will claim that they have the freedom to exploit information about the individual's media consumption by selling it to others—perhaps even the government.[9]

In a 2003 study of DRM-based content delivery technologies, Professor Deirdre Mulligan, John Han, and Aaron Burstein concluded that they engaged "in detailed surveillance of content consumption by consumers within private spaces. In most instances the systems monitor the content used, the time of use, the frequency of use, and the location of the use."[10] Specifically, Mulligan, Han, and Burstein found that:

> "Each of the services that we studied requires the local installation of proxy software. Use of MusicNet requires the additional installation of RealPlayer and America On-Line. While left active these software proxies continually reference Windows Internet Explorer (IE) index.dat files. Index.dat files serve as history logs for the folders in which they reside. One resides in each of IE's cookies, history, and temporary Internet files folders. These files are not affected when folder contents are altered or deleted, and cannot themselves be deleted. Thus, index.dat files act as a type of permanent record of the websites that users have browsed and of the files that they have downloaded from the Internet.
>
> "Rhapsody's software client contacts Rhapsody's content server every 45 seconds while idle. This software reads from Window's index.dat files prior to every transmission. Since there is no clear reason why the service, while idle, would require information about cookies or browsing history, these two findings in conjunction may reflect monitoring of user browsing habits.
>
> "The two film services require their customers to transact with servers to reacquire new license files each time content is rendered. Both MovieLink and CinemaNow state that they collect usage information concerning the number of times films are played for royalty purposes. The "registration" with services

[8] Press Release, SunnComm, Inc., *Sunncomm and Music City Records Agree to Resolve Consumer Music Cloqueing Law Suit by Providing Better Notice and Enhancing Consumer Privacy* (Feb. 22, 2002), at http://www.xenoclast.org/free-sklyarov-uk/2002-February/001580.html.

[9] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002).

[10] Deirdre K. Mulligan, John Han, Aaron J. Burstein, *How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use*," ACM DRM '03 Conference, Oct. 27, 2003, available at http://www.law.berkeley.edu/cenpro/samuelson/papers/other/p029-mulligan.pdf.

> servers each time films are played for the first time, paused and resumed, or rewound and resumed, no doubt allows the two movie services to maintain meticulous records concerning how movies files are used by individual customers. Windows Media Player may also be used to monitor how content files are used. WMP records the number of times individual tracks are rendered in order to enforce restrictions on track playback.
>
> "Furthermore, using the services studied initiates highly complex webs of information monitoring and exchange. For example, the number of advertising partners Pressplay engages with is unclear. However, it is clear that usage of the service involves interaction with a minimum of four separate entities with a minimum of four separate policies governing use of information collected about users. The other services examined all exhibit similar degrees of complexity.[11]

The authors concluded that: "As others have noted, Fair Information Practice Principles, particularly collection limitation, disaggregation of identifying and transactional data, and data destruction should inform the design and implementation of all aspects of DRM. In particular, DRM system developers should eschew the collection of data that is not absolutely necessary to protect content."[12]

As Mulligan, Han, and Burstein demonstrated in their study, Digital Rights Management systems can engage in invasive monitoring. These invasive activities occur with notice to the user, and with user consent. We think, therefore, that the Commission should not focus solely on notice and consent issues. A full set of Fair Information Practices should be used to evaluate DRM systems, and software traditionally defined as "spyware."

B. Distribution of Spyware

i. What role does peer-to-peer file-sharing play in the distribution of spyware?

When privacy issues are viewed from voluntariness and quality of consent lenses, it becomes clear that invasive technologies can be distributed from both "legitimate" and "illegitimate" commercial entities. Placing focus on peer-to-peer distribution systems is inappropriate. In fact, harm to the peer-to-peer model could ultimately enhance Internet surveillance. Peer-to-peer networks are being employed in other countries to evade government surveillance of communication and to promote free speech. New versions of peer-to-peer software will offer anonymous and encrypted communication, thus stymieing commercial and government snooping of speech and online activities. The Commission should not focus its inquiry on peer-to-peer as a primary source of invasive software. Instead, a broader view should be taken. The Commission should focus on whether the software exhibits indicia of invasiveness.

[11] *Id* at 5-6. (internal citations omitted).
[12] *Id*.

D. Possible Responses to Spyware Concerns

i. What can government do to prevent the harms related to spyware?

The European Commission's Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, in its January 1999 report entitled "Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware," addressed the issue of governmental response to spyware.[13] Recommendations of the Working Party include:

- The data subject should be informed of the processing performed on her computer by hardware and software.
- Internet users should be notified of the types of information that might be collected about them.
- Users should be given the capacity to access any data that has been collected about them.
- Computer configurations should not allow for the default collecting, storing, or sending of user activity (called "client persistent information" – examples of which are users surfing habits and other patterns of user activity).
- The user should have available to her, filter tools, to block or modify the reception, storage, or sending of "client persistent" information.
- "Client persistent" information should be easily removable from a computer.

We again urge the Commission to apply a full set of Fair Information Practices when addressing spyware and other software that collects personal information. Notice is not enough. Consent too, is not enough. There should be a floor of standards protecting privacy, because the market will not provide competition in this area to increase privacy. Instead, the price of access to desired content (in particular, movies and new music, which are usually held exclusively by one media company or another) will be conditioned on individuals' giving "consent" to operating invasive software like those described by Mulligan, Han, and Burstein.

Author Simson Garfinkel has suggested that the government adopt a "Pure Software Act" to address the scourge of spyware.[14] Garfinkel reasons that deception in notice drives the spyware problem, and thus, a pure-foods-like regulation could help individuals identify spyware.[15] Specifically, icons should accompany software that represent invasive monitoring or other indicia of spyware. The Commission should consider Garfinkel's proposal as one tool in combating spyware.

The Commission should determine to what extent, if any, software should be serialized. Serialization in software is a key tool for tracking, and accordingly, the Commission should view serialized software as invasive and potentially spyware.

---

[13] available at http://europa.eu.int/comm/internal_market/privacy/workingroup/wp1999/wpdocs99_en.htm.
[14] Simson Garfinkel, *The Pure Software Act of 2006*, Technology Review, Apr. 7, 2004.
[15] We note that the pure foods or nutrition label analogy is not appropriate for conceptualizing privacy notices. Food and drug regulation requires not only notice, but also a baseline of protections guaranteeing purity and safety. Even if a company provides notice and obtains consent from members of the public, it cannot market poisonous or harmful food. Notice is not enough for protection of food; neither is it enough for protection of privacy.

The Commission should continue its efforts to encourage users to employ virus protection, firewalls, and scanning software that can detect and remove spyware. However, the Commission's efforts should not be solely focused on preventative measures that can be employed by individuals. Individuals already have to navigate the privacy implications presented by cookies, thousands of privacy policies, opt-outs, etc. The Commission should consider whether it would be more efficient to establish norms for privacy protection that would act as a baseline for all, rather than the hodge-podge of self-help advocacy that confuses all but the most computer literate.

iv. Can industry best practices or self-regulation decrease consumer concerns about spyware? If so, how and to what extent?

The principles of spyware (and often, online profiling) contravene "best practices." From a privacy perspective, these practices violate the first Fair Information Principle—minimization. Furthermore, the Commission should consider the present self-regulatory environment may be responsible for the propagation of spyware. Indeed, if Internet users possessed statutory rights in their personal information, and data collectors had responsibilities to users, spyware may not have grown to be such a problem.

On a technical level, if Microsoft Windows were designed to give an individual more control over software, spyware may be more avoidable. Currently, spyware can propagate itself and respawn because it is easy to place keys in the Windows registry and to place programs in menus that are started at boot time. Many users cannot explore the registry, remove keys, or even receive notice when a new key is placed in a "run at boot" folder. Operating-level user control over the registry and boot menus could help prevent the spread of spyware.

Respectfully submitted,

Chris Jay Hoofnagle
Associate Director
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
202.483.1140 x108