

Spyware

INSIDE

Introduction	2
Spyware Infiltrates the Enterprise	3
Rogue's Gallery of Spyware	7
Time to Own the Spyware Problem	10
Doing the Spyware Shuffle	11
Industry Tries to Unite Against Spyware	12
A Defining Moment for Spyware EULAs	13
Government Focuses on Countering Spyware	15

Compliments of:

SOPHOS

Introduction

WHETHER YOU'RE REFERRING TO ADWARE — supposedly benign applications that users download in exchange for agreeing to see ads or provide marketing information — or the more dangerous spyware, unwanted software is running rampant in today's enterprises. More than 92 percent of IT managers polled said that some or all of their PCs were affected (or is that infected?). Although awareness of the social, technological, and security dangers of spyware is still growing, the damage is being done today — and spyware is evolving faster than countermeasures, as this IT Strategy Guide explains.

While vendors quibble about definitions, some of the best-known adware and spyware products are worming their way into your PCs, everywhere on your network. The CoolWebSearch utility, affiliated with more than 1,000 Web domains, exploits unpatched browser holes to install itself. When installed, it slows PCs, changes bookmarks, pops up ads for pornographic Web sites, and redirects search-engine queries.

Another popular non-favorite, Claria's GAIN (Gator Advertising Information Network), overlays ads onto Web pages, tracks what sites your employees are visiting, and causes crashes and impacts PC performance.

The dangers of spyware are growing as key loggers, phishing scams, and other malicious activities begin using this newer delivery method. You can't place your trust in individual end-users' decisions to install an anti-spyware tool. Just as with other security software — firewalls, anti-virus and anti-spam — it's time to choose a

centrally managed, policy-based solution.

The challenge is that there are few enterprise-ready tools to choose from, in part because there's little agreement as to exactly what spyware is and how to combat it. A new industry group, the Anti-Spyware Coalition, hopes to change that. However, such efforts have been tried before; a similar group, called the Consortium of Anti-Spyware Technology Vendors, fell apart earlier this year. For now, the spyware makers have the upper hand while the tech industry remains in disarray.

One weapon in the hands of the black hats isn't even technological. The EULA (end user license agreement) that many users blindly accept when downloading or installing new software apparently gives malware makers licenses to spy. That's why notorious purveyors, such as Claria, keep claiming that because users give their consent, their software isn't actually spyware at all. But your employees can't be relied upon to study the fine print and make the right decision every time they install or upgrade software. Something has to be done. But who will do it?

The "who" might be the government. As this guide explains, two bills focused on spyware passed the U.S. House of Representatives earlier this year. While not perfect, they may be steps in the right direction, especially because some of the challenges facing anti-spyware efforts may be legal, rather than technological. But no matter how we define the challenge, the truth remains: It's our job to fight it.

— Alan Zeichick

Spyware Infiltrates the Enterprise

DESKTOPS LITTERED WITH POP-UP ADS, COMPUTERS grinding to a halt under the weight of snoop software, private data snatched off networks and sent to a server somewhere in Siberia or San Francisco ... all these unfortunate occurrences can be attributed to spyware, a generic term for software that regularly collects demographic and usage information from a computer and transmits it to a marketing company or other interested parties without the user's explicit permission.

Spyware is far more intrusive than spam and can cause more real problems than many computer viruses. The more benign versions — sometimes called adware — confine themselves to downloading and displaying “targeted” ads and may only be resource hogs. But many spyware applications go farther. They auto-update themselves, alter system configurations, download and install additional software, and access and disclose data stored on computers they infect — or on any shared network resources that the affected computer can access.

ISP EarthLink offers subscribers a free spyware scanning service. Of the more than 2 million computers scanned between January and September of last year, one in three harbored spyware, with an average of 28 spyware programs per infected machine. Hardware vendor Dell says 12 percent of the support requests it receives concern spyware. Dell and EarthLink believe their respective support calls and scan requests come mainly from home or small-business users. Are enterprise networks spyware-free?

According to the results of a recent survey conducted on behalf of enterprise security vendor Secure Computing by independent research company TheInfoPro, only

25 percent of polled enterprise IT managers thought spyware was a major problem. That was not the response Tim McGurran, president and COO of Secure Computing, was expecting.

“Frankly, we were surprised that so few enterprises appear to be worried about spyware,” McGurran says. “Statistics definitely show that spyware is a serious problem in the enterprise. Equally disturbing was that the majority of the respondents also said that they have spyware policies in place in their organizations but that the policies aren't really enforced.”

Secure Computing's survey didn't ask IT managers whether spyware was or had been present on their systems. A recent poll by Harris Survey did ask, and 92 percent of polled IT managers said their organizations had been infected with spyware — with an average of 29 percent of their corporate PCs infected.

Because both surveys were conducted according to accepted rules of research, we're left with a conundrum: IT administrators admit a large percentage of enterprise computers have been infected and yet insist spyware isn't a real problem. Enterprise security vendors themselves have only recently begun to take spyware seriously, meaning that the best software for detecting and removing spyware still originates from a handful of small, relatively obscure software vendors.

“When a company loses a significant amount of money — or is the victim of a demonstrable case of corporate espionage — and it makes a major impact in the newspaper, then corporations will take notice,” says Bruce Schneier, founder and CTO of Counterpane Internet Security. “My guess is that this kind of thing is already

happening and will happen with a greater frequency in the future. Criminals, from lone criminals to organized crime, have discovered spyware.”

Spyware or Adware?

Businesses aren't ignoring the spyware issue, but it's not high on the agenda, says Kevin Harvey, senior technical consultant at technology consultancy Forsythe. “Part of the problem is that spyware isn't as well understood as other security risks,” he says.

The confusion over what spyware is — a plague from the darkest corners of the Internet or a nice software present with a small catch from the marketing world — and the slight but legally actionable difference between it and its less malicious sibling adware make it difficult to develop solutions and strategies to deal with the problem.

Claria, which distributes the Gator software that some refer to as spyware, last year filed a libel suit against an anti-spyware program vendor. The suit was settled out of court when PC Pitstop removed information critical of the company and its software from the PC Pitstop Web site. Claria insists that Gator is not spyware because the software's behavior is clearly explained in end-user licensing agreements and the people who use Gator software know they are providing their personal information in exchange for free software. Claria claims it currently “serves” more than 43 million consumers who have agreed to receive advertising.

Claria's argument was borne out during a recent security scan of an enterprise network by Blue Coat Systems, a company that manufactures proxy appliances that control how employees use the Internet. Blue Coat offers companies a free service called a Web Traffic Assessment. During an assessment, Blue Coat installs a proxy appliance onto the network without any policy controls, allowing the appliance to simply log all Web activity taking place on the network. Steve Mullaney, vice president of marketing at Blue Coat, says this has been very effective in helping some large

companies identify spyware on their networks.

“Blue Coat recently ran a Web Traffic Assessment for a large Fortune 500 enterprise manufacturing company and found out that the No. 1 visited Web site in corporation was Gator.com,” Mullaney says. “Management did not know what Gator was, and when we told them it was adware/spyware, they were shocked, to say the least.”

How did Gator get on those machines and drive that traffic? Because Blue Coat can pinpoint individual users, management asked some users whether they knew they had spyware/adware on their machines. Surprisingly, the users said yes, they did know. In fact, they had installed Gator and explicitly agreed to receive aggressively served ads in exchange for Gator's e-wallet application.

“After further probing by IT staff, one user says, ‘Well, I wouldn't install adware on my computer at home,’” Mullaney says. “The IT staff then learned that some of the users didn't want to slow down their home PC or home Internet connection with adware. The CIO was not amused.”

So Claria may be right — some users know what they're getting, and there may be some difference between adware and spyware. But does this matter to anyone but Claria and the people contacted by the company's lawyers? Some security experts say it does.

“It's necessary to understand the difference between adware and spyware when addressing how these programs are getting onto corporate networks,” says Gregg Mastoras, senior security analyst at Sophos, a security application vendor. “Adware is usually deliberately installed by a user. It is a noisy application, clearly announcing its presence on a computer through advertisements. You prevent it through policies and user education.”

But spyware, Mastoras says, is stealthier. “Spyware usually installs itself without permission via holes in software or doesn't come with a clear explanation of its purposes. Spyware is a subtle, under-the-radar application that wishes to remain unnoticed so that it can collect

data without interference,” he says.

Aggressive spyware variants pose a severe threat, particularly for companies that subsist on sensitive data. “I know of one major HMO that has a 10-person staff dedicated solely to the eradication of spyware because they feel it is such a risk to their HIPAA compliance,” says John Bedrick, group product marketing manager of system security at McAfee. “We also worked with a major financial institute that was hacked. User IDs and passwords were gathered by spyware and transmitted to a third-world country, and the company’s network was then hacked with remote administrative tools.”

Begone, Scum

So what strategies should enterprises use to fend off spyware and adware? As with any vexing problem that has security implications, the solution derives from a combination of policy and technology.

One approach is simply to jettison Internet Explorer. The majority of adware and spyware works only on computers running Microsoft’s operating system and Web browser. Some experts advise switching to the Mozilla’s Firefox Web browser to cut down on “drive-by installs” — that is, spyware that installs itself without users’ knowledge or explicit permission.

Security experts agree, however, that spyware is sneaking onto corporate desktops largely as a result of user behavior. “Spyware has many vectors, but the critical issue is that the door is opened by user actions. If end-users are allowed to install software and to freely browse the Web, the enterprise is exposed,” says Richard Stienon, who until recently was a lead security analyst at Gartner and is now vice president of threat research at Webroot Software, a security software vendor.

Policy enforcement should ensure that good users don’t do bad things such as installing silly programs on their desktops or running file-sharing applications that typically harbor a slew of spyware. And good patch management polices should prevent sneaky programs from

installing themselves on a computer without the user’s knowledge via security holes in operating systems and Web browsers.

Yet as Sophos’ Mastoras notes, “End-user behavior generally triumphs over protection, patching, and policies. Few organizations are able to actually enforce the policies they create.”

Factor in human behavior, and conventional security technologies alone aren’t up to the task. “Typical large enterprises have firewalls and anti-virus but lack protection at the application layer. More specifically, they lack HTTP protection, which most spyware uses as its primary mode of communication,” Blue Coat’s Mullaney says. “Firewalls have traditionally focused on ports and, to some extent, protocols but have no visibility into content. Furthermore, attempts to extend anti-virus scanning to HTTP historically have failed due to poor performance and false positives that resulted in poor Web experiences for the end-user.”

Enterprise anti-virus vendors such as McAfee, Sophos, and Symantec say they are bolstering their applications’ capabilities of blocking and/or removing spyware and adware. But vendors that offer targeted enterprise anti-spyware apps point out that their products provide a good complement to anti-virus applications, offering focused, comprehensive protection against a specific threat.

Unlike anti-spyware products designed for home users, enterprise editions are fully automated, sweeping the network for infestation however often IT chooses to set the program to scan (most vendors recommend a daily sweep). Spyware can be automatically removed or remotely quarantined, as an administrator chooses.

Enterprise anti-spyware applications such as Webroot Spy Sweeper Enterprise and PestPatrol Corporate also allow system administrators to fine-tune spyware protection by defining safe lists of applications that users can install or run, a feature not yet offered by anti-virus applications. Certain or all types of cookies can be permitted.

The applications can also inoculate networks, automatically blocking the installation of known spyware. Because one person's spyware is another's useful application, each company can configure auto-blocking to suit its enterprise.

"Good security requires defense in depth," Counterpane's Schneier says. "There's no 'benefits of inoculation vs. scanning' argument with spyware; a smart company does both. Security is always a trade-off, and companies always have to weigh the costs of loss vs. the costs of risk mitigation. In this case, it's a no-brainer. There are easy — and cheap — tools that drastically reduce the risk of spyware."

Counting on Countermeasures

Enterprises may find these tools preferable to draconian measures such as preventing users from installing any applications on their computers. Paul Bryan, director at Microsoft's security business unit, says that the company is addressing the core issues of deceptive software with the goal of ensuring that what's happening on an individual machine is recognized and controllable.

"Microsoft's new IE pop-up blocker is turned on by

default and cuts down on a key way consumers are enticed and tricked into downloading deceptive software. And unsolicited downloads are now blocked by default," Bryan says. "We also added additional group policy controls that allow administrators to block downloads in the intranet zone."

Bryan acknowledges, however, that "XP [Service Pack 2] is not the complete solution by any means. As with most security challenges, there is no silver bullet, but it represents the kind of technology solution that we believe will help all of our customers deal with the spyware problem."

Most security experts agree that Windows XP Service Pack 2 does a good job hardening its OS against spyware that installs without explicit user permission. And just in time, too. Security experts believe that spyware is quickly getting creepier and more capable.

"We are in the very early stages of spyware," Forsythe's Harvey says. "Spyware is likely to become even more stealthy and capture more information as current code is refined. I believe we will hear many horror stories in the coming months about confidential corporate information being divulged through spyware."

— *Michelle Delio*

Rogue's Gallery of Spyware

THESE SPYWARE AND ADWARE MISCHIEF-MAKERS have taken root on more than their share of hard disks. Symptoms include performance and compatibility problems, not to mention continuous pop-up invasions.

CoolWebSearch

Aliases: CWS

Actions: CWS has more than three dozen variants, with new variants being released almost weekly. Typically, CWS blocks access to popular search engines and redirects users to coolwebsearch.com or other off-brand search sites. Entering incorrect or incomplete URLs results in users getting redirected to adult sites or obscure search sites. It adds links — often to hardcore pornography sites — to browser favorites/bookmarks menus. It also pops up ads — again often for hardcore sites — and changes default start pages to adulthyperlinks.com, allhyperlinks.com, or other ad-heavy directories or adult sites.

Security issues: CWS program code is remotely updated, apparently from a server in Russia. Some variants add CWS' servers to Internet Explorer's Trusted Sites list, enabling program code — not limited to CWS code — to be installed or altered without permission. Some variants collect and transmit personally identifiable information back to CWS servers.

Other issues: CWS severely impacts infected computer's performance. Software may freeze or crash, especially Internet Explorer. IE performance is noticeably slowed, particularly page scrolling. Microsoft tech support has had reports of computers locking up, crashing, and rebooting repeatedly due to CWS issues.

Transmission method: More than 1,000 domains are known to be affiliates of CWS. Affiliates get paid per referral/click-through to coolwebsearch.com. Users visiting any one of the affiliate sites may install CWS software by careless clicking on a pop-up or other ad. CWS has apparently been installed without user knowledge or permission via unpatched IE security holes.

Xupiter

Aliases: OrbitExplorer

Actions: Xupiter launches pop-up ads, changes default home pages, redirects mistyped or incomplete URLs to affiliate sites, redirects search requests to off-brand search sites, and adds Xupiter links to bookmarks/favorites. Xupiter blocks any attempts to restore the original browser settings or to delete Xupiter favorites.

Security issues: Xupiter's privacy policy notes that Xupiter — or its partners — may deliver programming fixes, updates, and upgrades via automatic updates. "Users" are also advised that conflicts may occur with other applications and that Xupiter will determine what those applications are so that the company can resolve these conflicts whenever possible. Several versions of Xupiter appear to download other programs such as gambling games onto affected computers.

Other issues: Technical support representatives at Microsoft's help center say Xupiter has odd effects on Windows XP, making it impossible for some users to open directories such as My Computer on infected computers.

Transmission method: Xupiter is installed via an Internet Explorer toolbar program. Some users claim toolbar

was installed without their permission on unpatched versions of IE. Toolbar may be downloaded via Web sites, links in spam advertising a “Free Christian Toolbar” or a pop-up blocker program, or via links in pop-up ads.

Gator Advertising Information Network (GAIN)

Alias: Gator

Actions: Gator overlays ads onto Web pages, tracks what Web sites are visited by users, transmits information about products and services users are interested in, and monitors response to Gator-produced ads. This information is made available to advertisers.

Security issues: According to its privacy policy, Gator transmits information on system settings and configuration information — software installed on the computer, and more — as well as first name, country, city, five-digit ZIP code/postal code, and “non-personally identifiable information” entered into Web page forms, such as the first four digits of credit card numbers, which identifies the issuing bank but not the cardholder. Gator also auto-installs and/or updates other software components, such as rich media player applications, browser plug-ins, virtual machines, and run-time environments.

Other issues: Gator distributor Claria insists Gator is not spyware and has been involved in several court cases in attempts to prove this claim. Users report computers with Gator exhibit slowed performance and/or software crashes.

Transmission method: The Gator Advertising Information Network offers half a dozen applications that contain Gator, such as a desktop weather forecast program, a calendar, a computer clock synchronization program, the “Gator e-wallet,” and a program called Websecure Alert, which Gator documentation says “helps to protect your browser security by monitoring for unauthorized tampering with Internet Explorer’s security settings, and can help to protect your privacy by deleting your web surfing history on a regular basis.”

Live Online Portal (LOP)

Aliases: C2

Actions: This family of spyware applications reset user’s default start and search pages to lop.com or one of 200 Live Online Portal (LOP) affiliates such as ifiz.com, iguu.com, samz.com, sckr.com, scrk.com, and sfux.com. LOP resets start and search pages back to lop.com if user attempts to change them, adds shortcuts to advertisers’ sites on desktop and links in favorites/bookmarks, and adds new IE toolbar called Accessories, with yet more advertising links.

Security issues: LOP can download and execute arbitrary code from its server.

Other issues: Overall performance is slowed. Mobile users may get frequent dial-up connection requests if their computers are not online when LOP wants to perform some action. Computers may freeze for a few minutes after these connection requests are refused by user. LOP program may demand answers to series of riddles before allowing itself to be manually uninstalled. LOP program may demand answers to series of riddles before allowing itself to be manually uninstalled.

Transmission method: LOP’s most infamous installation method is to create pop-up loops (pop-ups opening pop-ups) featuring ads for MP3 search and download tools. One false or frustrated click in the midst of the pop-up plethora and the machine is infected. LOP has also been bundled as a legitimate music/software download search tool with various freeware software offerings.

Cydoor

Aliases: None

Actions: Cydoor produces the usual complement of pop-up ads and many pop-under ads.

Security issues: No security issues are known with recent versions of the software. Program seems to confine its connections with the mothership to updating ad cache, not programming code. Little if any personal information not directly supplied by user is captured.

The most recent versions of Cydoor are nearing the point where they can no longer quite be considered spyware.

Other issues: Users do not have to be online to view Cydoor-produced ads. Program pulls ads from cache (c:\Windows\System\adcache\) within affected computers. Cache is updated each time user goes online. Anti-spyware vendor PestPatrol reports numerous complaints of Cydoor causing system errors in Windows XP. **Transmission method:** Cydoor is widely distributed as a component of p-to-p programs, some freeware games, and other applications. Not offered as a stand-alone download.

Look2Me

Aliases: AllAboutSearch.com

Actions: Look2Me primarily displays pop-up advertising for clients. Pop-ups — some full-window size — can appear on screen every minute or so. Look2Me also

installs shortcuts on desktops and changes default browser settings. Some users of infected machines report that applications linked to shortcuts have been installed without permission. But tests of Look2Me on patched Windows 2000 and XP systems did not exhibit any capability of self-installing programs.

Security issues: Look2Me monitors Web sites visited and then submits this information to its home server. Look2Me auto-updates its code, and program components could run arbitrary code during this procedure.

Other issues: No significant performance issues have been noted, besides users being pelted with pop-up ads. IE may slow down. Look2Me will not show up as a running process or application as it tightly integrates itself with Internet Explorer, making it difficult to monitor and manage its activity.

— *Michelle Delio*

Time to Own the Spyware Problem

EARLIER THIS YEAR, FORRESTER RESEARCH released “Anti-Spyware Adoption in 2005,” a study by analyst David Friedlander with Natalie Lambert, that included some surprising stats. What struck me most was that 39 percent of respondents, dubbed “technology decision makers,” did not know the percentage of desktops infected with spyware in their organizations. Perhaps they didn’t know because 56 percent were unsure of what percentage of help desk calls were related to spyware issues.

IT departments cannot hide their heads in the sand. If you ease your conscience by telling end-users to install anti-spyware software, you are only fooling yourself.

The Forrester report says that, on average, 7 percent of all help desk calls are made in response to spyware infections; Dell’s own estimate is 20 percent.

As an exercise, take 7 percent of the number of support calls you received last month and multiply that by what you believe the average cost of a single call is. (Dell claims \$35 per call, on average.)

I spoke with Forrester’s Friedlander on this issue, and he didn’t paint a happy picture. Spyware, he says, is getting more prevalent — and more malicious — on desktops.

“The big thing with spyware is it is financially motivated, which is not usually true of viruses,” Friedlander says.

Although key loggers are being used to steal personal passwords and credit card numbers today, who’s to say they won’t be used for full-fledged corporate espionage tomorrow?

Andy Ostrom, director of marketing at InterMute, makers of SpySubstract Enterprise, also notes that browser-hijacking software is getting tougher to remove. If you don’t get every last bit of code, it comes back.

Scarier still, according to Ostrom, InterMute has seen phishing attacks move from e-mail into spyware. A spyware application might pop up a dialog that warns you of a problem with your account only to redirect you to a look-alike site.

Steve Workman, director of product management at LANDesk Software, says that fobbing off the problem to the end-user is extremely shortsighted. Relying on end-users to decide what is and isn’t spyware doesn’t really protect the organization. And, as any IT manager knows, just having end-users install an application can turn into a disaster. Imagine 10,000 users clogging up the network by installing individual anti-spyware applications and downloading spyware definitions.

LANDesk Security Suite centralizes spyware definitions and updates in one spot. LANDesk’s subscription service keeps an up-to-date content list of new spyware definitions as they become known and sends customers updates.

LANDesk, as it turns out, is mostly owned by Intel. Workman tells me his company is participating with the giant chipmaker in its Active Management Technology initiative, which will provide management capabilities at the chip level, allowing IT to manage a device before the OS loads. For example, if policy dictates that a machine needs to be at a certain patch level, Active Management will keep spyware under control even before the machine is logged on to the network.

Nevertheless, you can’t let Intel or end-users fight your battles for you. It’s up to IT to take charge of the spyware problem now before it morphs from an annoying end-user problem into a full-blown corporate crisis.

— *Ephraim Schwartz*

Doing the Spyware Shuffle

WALKING AROUND INTEROP THIS YEAR, I SOMETIMES had to check my badge to see where I was. No, it wasn't just the talking stuffed camels in the lobby of my hotel — the Egyptian-themed Luxor — that made me think I was in some Bob Hope-Bing Crosby bad road-movie dream. It was also all the security products on display.

The Wireless Pavilion in particular seemed full of security products, as vendors seek to plug the latest hole to spring a leak in corporate networks. Even during John Chambers' keynote, the Cisco CEO harped on security. According to Chambers, security was the top issue among CTOs and CIOs Cisco surveyed.

There was some pretty good evidence this week as to why IT managers are so concerned about security. The State of Spyware Report (see infoworld.com/3004) from Webroot showed that, in the first quarter of 2005, 88 percent of Spy Audit scans found some form of unwanted program (Trojan, system monitor, cookie, or adware) on consumer computers.

Believe it or not, that is down slightly (by 1 percent) from the fourth quarter last year. Research from the report also indicates that various forms of spyware — pop-ups, home-page hijackers, search redirection, and host file and DNS poisoners — generate an estimated \$2 billion in revenue annually. These numbers indicate that this previously unmeasured market may be approaching 25 percent of the already established market of online advertising as reported by the Internet Advertising Bureau, according to Richard Stiennon, Webroot's vice president of threat research.

“Our research shows that some form of spyware, adware, or potentially unwanted software can be found on 87 percent of corporate PCs. This figure is disconcerting from a security perspective and also from an IT support perspective, as spyware can often slow down the performance of an entire network,” Stiennon said.

The Webroot report also examines recent incidents of real spyware exploits that have crippled some enterprises, including the attempted multimillion-dollar theft from a major international financial institution by a hacker using a planted keylogger.

If you aren't a Green Day American Idiot and if you think you're not that involved in corporate computing because you steer clear of the Windows operating environment, that doesn't mean you're immune from attack. A report from the SysAdmin, Audit, Network, Security (SANS) Institute (see infoworld.com/3005) says that versions of iTunes prior to 4.7.1 can be exploited on both Windows and Mac platforms.

It's not good news, but at least it's not a talking stuffed camel.

— *Bob Francis*

Industry Tries to Unite Against Spyware

THE ANTI-SPYWARE COALITION (ASC), A GROUP OF IT companies and public interest groups, is hoping to succeed where a previous vendor organization failed in tackling the global problem of spyware. The ASC released an agreed-upon draft definition of spyware in July that it hopes will promote public comment and ultimately result in users becoming better educated about the dangers of spyware.

The Consortium of Anti-Spyware Technology Vendors (Coast), initially drawn from the security software vendor community, fell apart in February after a failed 16-month effort to coordinate its members' conflicting goals and an ongoing debate over admitting companies that created spyware. The ASC, convened by the Center for Democracy and Technology, has a much wider membership than Coast.

ASC members include the likes of America Online, Computer Associates International, Hewlett-Packard, Microsoft, and Yahoo, along with McAfee, Symantec, and Trend Micro, and antispyware specialist vendors Aluria Software and Webroot Software. The organization also numbers the Canadian Internet Policy and Public Interest Clinic, the Cyber Security Industry Alliance and The University of California Berkeley's Samuelson Law, Technology & Public Policy Clinic among its members.

Ari Schwartz, associate director of the Center for Democracy and Technology, has been heading up the ASC's work.

The documents released by the ADC include a list of spyware and other potentially harmful technologies

aimed at users, a glossary defining commonly used terms relating to spyware and safety tips about how to protect against spyware. There's also a process laying out how to resolve disputes if a vendor believes its software has been wrongly tagged as spyware.

Spyware can be defined two ways, according to the ASC. "In its narrow sense, spyware is a term for tracking software deployed without adequate notice, consent or control for the user," the organization states in its glossary. However spyware is also used as an umbrella term encompassing not only its narrow definition, but also other "potentially unwanted technologies," the ASC adds, including harmful adware, unauthorized dialers, rootkits and hacker tools.

In its antispyware safety tips document, the ASC has six major recommendations for users to defend themselves against spyware. The organization suggests that users keep the security on their computers up to date; only download programs from Web sites they trust; familiarize themselves with the fine print attached to any downloadable software; avoid being tricked into clicking dialog boxes; beware of so-called "free" programs; and use antispyware, antivirus and firewall software.

— *China Martens*

A Defining Moment for Spyware EULAs

AT THE HEART OF THE SPYWARE PROBLEM LIES THE question of what constitutes proper notice and consent. As we all know, spyware purveyors claim the right to do anything as long as they give “notice” of what their software actually does somewhere in a long EULA, and their victim gives “consent” by clicking OK without reading it. So it seems a little strange to me that the Anti-Spyware Coalition would ignore this issue in its initial draft of spyware definitions.

The Anti-Spyware Coalition — a rather imposing collection of software companies and public interest groups - recently released the first draft of its Spyware Definitions consensus document designed to give anti-spyware vendors standard categorizations of unwanted software. While a noble effort, I was somewhat disappointed that the document didn’t at least take a stab at defining what proper notice and consent of spyware ought to be. After all, it’s the lack of a consensus on that issue that has stymied legislative attempts to come up with an effective anti-spyware law, so it would seem like one of the first issues the coalition would need to deal with.

It’s not that the document ignores the problem of spyware EULAs altogether. In fact, one of the defined terms is EULA:

“End User License Agreement (EULA): An agreement between a producer and a user of computer software that specifies the parameters of use granted to the user. The software producer specifies these parameters and limitations on use, which can become part of a legally binding contract. Some companies use the EULA as the sole means of disclosure of a program’s behaviors or bundling.”

In a similar vein, the document’s “Anti-Spyware Safety Tips” section for consumers includes a warning to read all the fine print:

“Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes important information such as aggressive installs or the inclusion of unwanted software in a given software installation is documented, but it may be found only in the EULA. The fine print may be the only place consumers can find notice of potentially unwanted technologies. Unfortunately, careful consumers must read all the fine print.”

Well, that’s true enough, of course, but it’s also completely useless advice from the point of view of dealing with spyware. If everyone would read and understand every 10,000-word spyware EULA and privacy policy, there wouldn’t be a spyware problem. There wouldn’t be much of anything, because we’d all be too busy reading all the EULAs and all the privacy policies that we’re confronted with every day. After all, you don’t know it’s a spyware EULA until you’ve read it.

Since Microsoft, Symantec, and some other big supporters of the sanctity of the EULA are members of the coalition, I suppose it’s not really surprising that the definitions leave the impression that spyware EULAs are perfectly valid. The software industry is conflicted over spyware EULAs because spyware companies aren’t the only ones who like to hide the real nature of the deal deep in the fine print. If spyware vendors are required to give real notice and get real consent, so might others in the technology business.

The simple fact is that the sanctity of the EULA is going to have to take a hit if the spyware plague is ever to be brought under control. Consumers can't and won't read all the fine print - they need real notice of what they're dealing with so they can give true consent. And if the Anti-Spyware Coalition is to be any more effective than previous industry-led attempts to curb the spyware menace, it's going to have to start by defining what that really means.

— *Ed Foster*

Government Focuses on Countering Spyware

TWO BILLS FOCUSING ON SPYWARE OVERWHELMINGLY passed the U.S. House of Representatives earlier this year, including one that requires many software programs collecting personal information to get permission before doing so.

The Securely Protect Yourself Against Cyber Trespass Act, or Spy Act, also would outlaw the act of taking over a computer in order to send unauthorized information or code, and diverting a Web browser without the permission of the computer owner. The bill, which passed the House by a vote of 393-4, prohibits Web advertising that computer users cannot close “without undue effort” or without shutting down the computer, and it prohibits collecting personal information through keystroke logging.

A second bill, the Internet Spyware Prevention Act, or I-Spy Act, sets jail terms of up to five years for a person who uses spyware to access a computer without authorization and uses the computer to commit another federal crime. The I-Spy Act also would allow a jail term of up to two years for a person who uses spyware to obtain someone else's personal information or to defeat security protections on a computer with the intent of defrauding or injuring the computer owner.

The I-Spy Act, sponsored by Virginia Republican Representative Bob Goodlatte, passed the House by a vote of 395-1. Both bills would have to pass the U.S. Senate and be signed by President George Bush to become law. Both bills passed the House in October, but failed to make it through the Senate.

The Spy Act, sponsored by California Republican Representative Mary Bono, would allow fines of up to \$3 million for spyware-like activity such as delivering unauthorized software to a computer or hijacking a Web browser. Security software updates are exempted from the Spy Act.

Unlike an older Bono bill, this version of the Spy Act doesn't attempt to define spyware, but outlaws several actions commonly associated with spyware.

An earlier Bono spyware bill, introduced in July 2003, broadly prohibited and defined spyware. Some software vendors, including those that market antivirus update software, objected that the definition was overly broad and could subject their services to fines.

Microsoft issued a statement praising both new bills as providing “important tools in the battle against spyware and other deceptive software.” But Microsoft also called for the Senate to include language that would protect vendors of antispyware software from lawsuits by companies distributing spyware. Two antispyware companies have been sued by firms asking that their software not be removed from users' computers, with Claria, a distributor of pop-up advertising formerly known as Gator, filing a lawsuit against PC Pitstop in September 2003. This year, Claria also asked Computer Associates International to stop its PestPatrol software from deleting Claria ad-targeting software, but CA refused.

Microsoft released its own Windows AntiSpyware software in January. “In its current form, these bills leave companies that are responding to consumer demand for

strong antispyware tools vulnerable to frivolous lawsuits brought by the very companies responsible for the proliferation of spyware and other deceptive software,” Jack Krumholtz, managing director of federal government affairs for Microsoft, said in a statement.

Others, including the libertarian think-tank Cato Institute, have opposed the spyware legislation, saying it's unneeded because the U.S. Federal Trade Commission (FTC) already has the authority to seek fines for deceptive business practices.

The new version of the Bono bill requires that creators of software that collects personal information get permission from computer users before installing the software. The consent requirement, however, has an exemp-

tion for Web sites tracking their own pages visited. The bill also gives the FTC authority to allow some software vendors to ask for permission only once, not every time their programs access a computer.

Bono's bill would also preempt any state spyware laws.

“As this nation continues to push towards a global e-commerce marketplace, spyware stands to undermine the security and integrity of e-commerce and data security,” Bono said in a statement. “Daily web activities by consumers have become stalking grounds for computer hackers through spyware. Consumers have a right to know and have a right to decide who has access to their highly personal information that spyware can collect.”

— *Grant Gross*