Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC

Hearing on

"Impact and Policy Implications of Spyware on Consumers and Businesses"

Before the

United States Senate Committee on Commerce, Science and Transportation

June 11, 2008
Room 253, Russell Senate Office Building
Washington, DC

Senator Pryor, Chairman Inouye, Senator Stevens and Members of the Committee, thank you for the opportunity to testify today on the topic of Spyware and S. 1625, the Counter-Spy Act. My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C. EPIC was founded in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC recently filed a complaint at the Federal Trade Commission on the specific problem of commercial spyware.[1]

Spyware, adware, and other information collection techniques are a growing threat to the privacy of Internet users. Computer users have noticed the effects. Ninety percent of users say they have adjusted their online behavior out of fear of falling victim to software intrusions.[2] The Webroot automated threat research tool has identified more than half a million different potential malware sites since January 2005.[3] Spyware can cause significant degradation in system performance, result in loss of Internet access and impose substantial costs on consumers and businesses.[4] Spyware can assert control over the operation of computers.[5] The privacy risks of spyware include the theft of private information, monitoring of communications and tracking of an individual's online activity.[6]

Importantly, privacy threats are growing not just in numbers, but also in type. Traditional spyware, adware and tracking cookies are now joined by other threats such as mobile device spyware,[7] "stalkerware," and the potential for social networking applications to function as spyware. Spyware comes from several sources including online attackers, organized crime, marketing organizations and trusted insiders.[8]

A new motivation for the cyber criminal is that spyware has become a profitable

---

[1] Complaint, Request for Investigation, Injunction and Other Relief, *In the Matter of Awarenesstech.com, et al*. (March 6, 2008), http://epic.org/privacy/dv/spy_software.pdf.
[2] Pew Internet & American Life Project, *Spyware: The Threat of Unwanted Software Programs is Changing the way People use the Internet*, 2 (July 2005), *available at* http://pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf [hereinafter PEW Spyware Report].
[3] Webroot, *State of Spyware Report Q2*, (2006), *available at* http://www.webroot.com/pdf/2006-q2-sos-US.pdf.
[4] Fed. Trade Comm'n, *Spyware Workshop - Monitoring Software on your PC: Spyware, Adware, and other software*, 8 (Mar. 2005) *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.
[5] *Id.* at 9.
[6] *Id.*
[7] Joseph De Avila, *Do Hackers Pose a Threat to Smart Phones?*, THE WALL STREET JOURNAL, D1, May 27, 2008, *available at* http://online.wsj.com/article/SB121184343416921215.html?mod=todays_us_personal_journal.
[8] Aaron Hackworth USCERT, *Spyware*, 3 (2005) *available at* http://www.us-cert.gov/reading_room/spyware.pdf.

business.[9] Individuals can also deploy spyware against each other.[10] Some ISP's have also begun to install their own spyware-like services.[11]

These threats require vigorous policy response. Policy must be able to innovate to recognize new challenges while substantively protecting consumer privacy.

Notice and Consent Schemes Do Not Adequately Protect User Information.

Ultimately, users must be able to control how and when information about them is used, disclosed and held. Solutions which rely on simple notice and consent will not adequately protect users. A recent survey of California consumers showed that they fundamentally misunderstand their online privacy rights.[12] In two separate surveys almost 60% of consumers incorrectly believed that the presence of "privacy policy" meant that their privacy was protected.[13] In a different survey, 55% of participants incorrectly believed that the presence of a privacy policy meant that websites could not sell their address and purchase information.

Users also routinely click through notices. The Pew Internet and American Life Project found that 73% of users do not always read agreements, privacy statements or other disclaimers before downloading or installing programs.[14] In such an environment, merely giving notice to users before the collection of sensitive information from their computers fails to adequately protect privacy in the way consumers expect.

Consumer data should instead receive substantive protection. Information should be kept securely, and users should have the ability to know what data about them is being kept, who it has been shared with, and to withdraw consent for the holding of this data. Further, data should only be collected and kept for specified purposes.

Important security information should also receive protection, even if it does not identify a user. The Counter-Spy Act places conditions on software that collects information such as the user's Social Security number and driver's license number. It also protects as "sensitive personal information" information such as financial account

---

[9] *See* Guillaume Lovet, *Dirty Money on the Wires: The Business Models of Cyber Criminals*, (2006), *available at* http://www.momindum.com/ressources/produits/fortinetFlash/content/_libraries/_documents/index1/GL_Business_Models_of_Cybercriminals.pdf.

[10] EPIC, Personal Surveillance Technologies (May 2008), http://epic.org/privacy/dv/personal_surveillance.html.

[11] Saul Hansell, *Charter Will Monitor Customer's Web Surfing to Target Ads*, THE NEW YORK TIMES, May 14, 2008, http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/.

[12] Joseph Turow, Deirdre Mulligan, and Chris Jay Hoofnagle, Consumers Fundamentally Misunderstand the Online Advertising Marketplace (Oct. 2007), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf.

[13] *Id.* at 1.

[14] Pew Spyware Report, *supra* note 2, at 6.

numbers when combined with passwords or other security codes.[15] Password and access information to other accounts, such as email or social networking, are not included.

EPIC recommends that strict protection be afforded to security information, such as username/password pairs, encryption keys, biometric data, or other access control information. The mining of this information may not lead directly to identity theft and other financial harm, but facilitates its spread. Gaining access to a user's non-financial accounts allows further information to be collected and further crimes perpetrated. Compromised accounts may have valuable information stored in them or be used to originate further malware attacks, including by impersonating the compromised account.

Privacy Requires Strong and Innovative Enforcement

EPIC supports giving the FTC the ability to seek treble fines and penalize pattern or practice violations, as section 7 of the Counter-Spy Act does. These changes will improve the FTC's effectiveness in pursuing repeat offenders, and also change the economic incentives and disincentives for purveyors of spyware.

Several states are using innovative policies to protect their citizens' privacy. Spyware legislation has been passed in several states, including Alaska[16], Arizona[17], California[18], Florida[19], Georgia[20], Illinois[21], Indiana[22], Iowa[23], Louisiana[24], Nevada[25], New Hampshire[26], Rhode Island[27], Texas[28], Utah[29], and Washington.[30] The Utah statute, for example, makes provision for a private cause of action which may be brought by a mark owner who does business in Utah and is directly and adversely affected by the violation.[31] In such a suit a mark owner may recover the greater of 500 dollars per each ad displayed or actual damages.[32]

State Attorney's General have pursued spyware providers under state spyware

---

[15] S. 1625, 110th Cong. § 12(13)(B) (2008).
[16] Alaska Stat. §§ 45.45.792, 45.45.794, 45.45.798, 45.45.471 (2007).
[17] Ariz. Rev. Stat. § 44-7301 to -7304 (2008).
[18] Cal. Bus. & Prof. Code § 22947 (2008).
[19] Fla. Stat. § 934.02, .03, .06 (2008).
[20] Ga. Code Ann. § 16-9-152, -157 (2008).
[21] 720 Ill. Comp. Stat. 5/16D-3 (2008).
[22] Ind. Code. § 24-4.8-1 to -3 (2008).
[23] Iowa Code § 715 (2008).
[24] La. Rev. Stat. Ann. § 51:2006-14 (2008).
[25] Nev. Rev. Stat. Ann. § 205.4737 (2007).
[26] N.H. Rev. Stat. Ann. § 359-H:1-6 (2008).
[27] R.I. Gen. Laws § 11-52.2-7 (2008).
[28] Tex. Bus. & Com. Code § 48.001-4, .051-057 (2008); Tex. Bus. & Com. Code § 324.001-7, .051-055, .101-.102 (2008).
[29] Utah Code Ann. § 13-40-101 to -401 (2008).
[30] Wash. Rev. Code § 19.270.010-.080, .900 (2008).
[31] Utah Code Ann. § 13-40-301.
[32] *Id.*

laws. Washington State successfully applied the Washington State Computer Spyware Act[33] (Spyware Act) to stop Secure Computer's use of their free computer scan that always detects spyware leading to instructions to buy their Spyware Cleaner product in a $1,000,000 settlement.[34] The State alleged violations under the state's Spyware Act, federal and state spam laws, and the state Consumer Protection Act.[35] The Attorney General's Office accused the company of "falsely claiming computers were infected with spyware" to entice the consumer to pay for their program that claimed to remove it.[36] The settlement required the company to inform consumers of their right to a refund and pay a $1,000,000 judgment.

For these reasons EPIC recommends that the Counter-Spy act not preempt state laws and state enforcement actions, as section 11(b) does. Federal law should set a baseline of privacy protection. It should not cap it.

EPIC recommends that the limitation in section 6(a)(10) be removed. The Counters-Spy Act's liability limitations broadly permit monitoring of users' computers and personal information for the " detection or prevention of the unauthorized use of software fraudulent or other illegal activities."[37] These limitations should be scaled back. The determination of whether uses are unauthorized, fraudulent or illegal may be complicated.

Privacy Threats Beyond Traditional Spyware Programs

Information collection online is not performed solely with spyware programs executed on user's computers. Third-party and opt-out cookies present growing threats. The proliferation of mobile devices means a potential new place for spyware to act. Internet service providers are begging to deploy their own adware and profiling services in ways which users will find difficult, if not impossible, to detect. Important user information is leaving the desktops and instead is residing on online social networking profiles. This information includes sensitive personal information such as contact information, one's social and business relationships, political interests, sexual orientation, as well as the contents of communications. Further, online social networking sites are increasing their own information collection practices.

A "cookie" is information about a particular user's identity and browsing

[33] Wash. Rev. Code § 19.270.010-.080, .900.
[34] State of Washington v. Secure Computer, LLC, No. C06-0126RSM (W.D. Wash. Nov. 30, 2006) (Consent Decree as to Defendants Secure Computer, LLC and Paul E. Burke), http://www.atg.wa.gov/uploadedFiles/Another/News/Press_Releases/2006/SecureComputerConsentDecree112906.pdf.
[35] Press Release, Washington State Office of the Attorney General, Attorney General McKenna Announces $1M Settlement in Washington's First Spyware Suit (Dec. 4, 2006), *available at* http://www.atg.wa.gov/pressrelease.aspx?id=5926.
[36] *Id.*
[37] S. 1625, 110th Cong. § 6(a)(10) (2008).

behavior that Web servers store on his computer, typically without his consent.[38] Cookies permit a user to customize his interface with a particular website, for example by automatically entering his username and password.[39] However, since cookies can match an individual user to his interests and browsing habits, they are increasingly placed, gathered, and exploited by advertisers and others with a commercial interest in precisely targeting ads and services.[40] Anyone with access to that user's cookies can track his browsing history and gather information about his behavior and identity.[41] As a result, Internet users who are concerned about privacy are widely encouraged to routinely purge the cookies they have accumulated or to refuse cookies from Web sites that require them.[42]

The recent Google-Doubleclick merger raises significant privacy issues because of the planned merger of the Google search engine database with Doubleclick's extensive data collection accomplished with third-party cookies.[43] EPIC filed a complaint with the FTC urging the Commission to impose privacy protections upon the merger, concluding:

> Google's proposed acquisition of DoubleClick will give one company access to more information about the Internet activities of consumers than any other company in the world. Moreover, Google will operate with virtually no legal obligation to ensure the privacy, security, and accuracy of the personal data that it collects. At this time, there is simply no consumer privacy issue more pressing for the Commission to consider than Google's plan to combine the search histories and web site visit records of Internet users.[44]

In November 2007 Facebook launched its Beacon service.[45] Beacon collects information from Facebook users when engaged in actions on other websites. Facebook then uses this information to broadcast advertisements to that user's friends on Facebook, alerting them of the actions that the user took on these other websites. Initially, Facebook only provided a brief opportunity for an opt-out. Facebook later added an opt-in system, and the option to globally opt out of Beacon. Shortly after Beacon's launch, security researchers showed that Facebook is receiving information even from those who are not logged in to Facebook and are not Facebook members.[46]

---

[38] Cookiecentral.com, The Cookie Concept, http://www.cookiecentral.com/c_concept.htm (last visited June 6, 2008)
[39] Cookiecentral.com, Purpose of Cookies: The Cookie Controversy, http://www.cookiecentral.com/ccstory/cc2.htm (last visited June 6, 2008)
[40] *Id*.
[41] EPIC, Cookies, http://epic.org/privacy/internet/cookies/.
[42] EPIC, Does AskEraser Really Erase?, http://epic.org/privacy/ask/default.html.
[43] *See* EPIC, Privacy? Proposed Google/DoubleClick Deal, http://epic.org/privacy/ftc/google/
[44] EPIC Complaint, *In the Matter of Google Inc. and DoubleClick Inc*., 10 (April 20, 2007), http://epic.org/privacy/ftc/google/epic_complaint.pdf.
[45] Facebook Beacon, http://www.facebook.com/business/?beacon.
[46] CA Security Advisor, *Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking Users Who Opt Out or Are Not Logged In*, (Dec 3, 2007), http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-

Users of social networking sites are also exposed to the information collection practices of third party social networking applications. On Facebook, installing applications grants this third party application provider access to nearly all of a user's information.[47] Significantly, third party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user's friends and network members that the user can see. This level of access is often not necessary. Researchers at the University of Virginia found that 90% of applications are given more access privileges than they need.[48]

These features may be exploited and the information used for other purposes. Investigators at the BBC took three hours to write an application that collected information that had been marked as unable to be shared with friends.[49] Facebook, as part of its response, cautioned that users should "employ the same precautions while downloading software from Facebook applications that they use when downloading software on their desktop."[50]

Mobile device spyware also presents a future privacy threat, with unique features due to the mobile environment. In December of 2006, McAfee reported on a new kind of mobile phone spyware, called SymbOS/Mobispy.A.[51] SymbOS/Mobispy.A installed on phones and recorded incoming and outgoing SMS messages.[52] It also tracked the phone numbers of all dialed and received calls. Mobile tracking presents unique dangers because it allows the tracker to determine the user's location. While the data may be able to follow users anonymously it may also easily identify them - they are likely at home in the evenings. Location information should receive significant protection from tracking applications.

A new more insidious form of adware has been tested in the United Kingdom, and at least one US company has announced it will also use the system.[53] British Telecom contracted with the former adware company Phorm to create secret profiles of its users.[54] Users' traffic was routed via Phorm boxes, which replaced ads on the pages users were

---

misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx.

[47] EPIC, Facebook Privacy, http://epic.org/privacy/facebook/.

[48] Privacy Protection for Social Networking APIs, http://www.cs.virginia.edu/felt/privacy/ (last visited June 6, 2008).

[49] Press Release, BBC, *Facebook's loophole places personal profile data at risk – BBC investigation* (May 1, 2008), http://www.bbc.co.uk/pressoffice/pressreleases/stories/2008/05_may/01/click.shtml

[50] *Q&A: Facebook Response*, BBC, May 1, 2008, http://news.bbc.co.uk/2/hi/programmes/click_online/7375891.stm

[51] McAfee Avert Labs Blog, http://www.avertlabs.com/research/blog/?p=145 (last visited June 5, 2008)

[52] *Id.*

[53] *See* EPIC, Deep Packet Inspection and Privacy, http://epic.org/privacy/dpi/.

[54] Chris Williams, *BT and Phorm secretly tracked 18,000 customers in 2006*, THE REGISTER, April 1, 2008, http://www.theregister.co.uk/2008/04/01/bt_phorm_2006_trial/.

visiting with its own targeted ads. In the US, Charter communications announced that it will monitor consumers' browsing in order to serve them targeted ads.[55] Charter sent several of its users cryptic notices of an "enhancement" to their web browsing experiences.[56] The letter pointed users to a website with more details, including the claim that "[t]here is no application downloaded onto a user's computer and, therefore, there is no "adware" or "spyware" on your computer from Charter in this enhanced service."[57] Thus a system that is functionally equivalent to spyware, and more dangerous due to its undetectability, is touted as safer because it does not reside on the victim's computer.

Finally, some companies market spyware directly for consumers to use for stalking and other criminal activities. These technologies are promoted to consumers to spy on email and instant message exchanges, record websites visited, and capture passwords and logins. EPIC has filed a complaint with the FTC against such "Stalker spyware," highlighting the unfair and deceptive practices used to market this software.[58] These practices include the promotion of illegal surveillance targets, the promotion of "Trojan Horse" email attacks, and the failure to warn purchasers of the legal consequences of illegal use.

We hope the FTC will take action on this complaint and take action against these firms.

Conclusion

Privacy online continues to face many threats, both from criminal entities as well as intrusive commercial ventures. Substantive consumer protections and innovative enforcement strategies are necessary to protect consumers from the evolving threat of information collection online. These threats include not just traditional spyware, but also the merger of online consumer databases, new social networking features, mobile spyware and stalker spyware.

EPIC recommends passage of Counter-Spy Act in line with the changes pointed out above. The Counter-Spy Act should not preempt state law or enforcement; it should protect important security information like username / login pairs; and the liability limitations should be narrowed. Congress should also be aware of other developing threats to privacy beyond traditional spyware programs.

---

[55] Saul Hansell, *Charter Will Monitor Customers' Web Surfing to Target Ads*, THE NEW YORK TIMES, May 14, 2008, http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/.

[56] Charter Letter, *available at* http://www.epic.org/privacy/dpi/subscriber_ltr.pdf.

[57] Charter Communications, Enhanced Online Experience Frequently Asked Questions, http://connect.charter.com/landing/op1.html#6.

[58] Complaint, Request for Investigation, Injunction and Other Relief, *In the Matter of Awarenesstech.com, et al*. (March 6, 2008), http://epic.org/privacy/dv/spy_software.pdf.