Testimony of Benjamin Edelman

before the

United States Senate
Committee on Commerce, Science and Transportation

June 11, 2008

Benjamin Edelman
Assistant Professor
Harvard Business School

Baker Library 445
1 Soldier's Field Rd
Boston, MA 02163

Chairman Inouye, Senator Pryor, Members of the Committee:

My name is Benjamin Edelman. I am an assistant professor at the Harvard Business School, where my research focuses on the design of electronic marketplaces, including designing online marketplaces to assure safety, reliability, and efficiency. My full biography and publication list are at http://www.benedelman.org/bio and http://www.benedelman.org/publications .

Today the committee considers the important problems of Internet spyware and deceptive adware – scourges that threaten the reliability, trustworthiness, and overall utility of many users' Internet's access.

My bottom line:

Despite some recent progress, spyware and adware continue to present substantial harms to Internet users and to the Internet as a whole.

Many improper practices are already prohibited under existing statutes including the FTC Act, state consumer protection statutes, and state anti-spyware legislation. These statutes have given rise to a series of cases, both public and private, that have somewhat reined in the problems of spyware and adware.

Tough Federal legislation could assist in bringing spyware and adware purveyors to justice, and in further deterring creation and support of this noxious software.

But the bill at hand addresses only a portion of the problem, while in some ways reducing the effectiveness of existing efforts. By prohibiting specific individual practices, the bill invites perpetrators to comply with the letter of the law while continuing to harm and deceive consumers. Moreover, perpetrators are likely to boast of compliance – despite offering software no reasonable user would want. These loopholes are inevitable in the bill's "laundry list" approach, which unavoidably omits deceptive schemes not yet invented.

Pages five and six set out my detailed suggestions for revision. I favor a rewrite that emphasizes consumer protection fundamentals such as a consumer's right to know what software runs on his PC, and to grant or deny consent to each program that asks to be installed. But the FTC has already established these principles through its existing anti-spyware litigation. Thanks to existing legislation plus the FTC's work to date, this bill can accomplish its apparent purpose without adding new prohibitions. Instead, this bill can grant the FTC discretion to seek increased penalties under existing statutes – sparing this committee the challenging task of deciding exactly what practices to prohibit.

The Consumer Victims of Spyware and Adware

Discussion of spyware and adware typically seeks, in the first instance, to attempt to protect the users who receive such software. After all, a computer with spyware or adware is often virtually crippled – filled with so many popups that doing other work is impossible or

impractical, and slowed so dramatically that it is unappealing to use the computer for ordinary purposes. Legislation and enforcement can help prevent such damage.

Adware vendors often claim their software arrives on users' computers only after users agree. As a threshold matter, my hands-on testing has repeatedly proven that adware can become installed without a user's consent.[1] But even if a user did accept the software, adware popups can nonetheless present substantial concern. For example, some adware popups are sexually-explicit – sometimes appearing without any obvious way to close the resulting windows to remove the explicit images.[2] Other adware popups resort to deception to try to sell their wares – combining the interruption of popups with the trickery of false advertising.[3] Moreover, adware popups appear separate from the programs that caused them – making it hard for users to understand where the ads came from, why they're there, and how to make them stop.

Users face a variety of costs in restoring a computer to good working order after an infection of spyware and/or adware. Some users hire technicians to make appropriate repairs. Others buy anti-spyware software. Furthermore, during the period in which spyware or adware impair a computer's operation, the user loses some or all access to the system he or she has paid for. These are real and troubling costs – out-of-pocket expense, lost time, and reduced productivity.

These harms are not outweighed by any countervailing benefits. Rare is the user who receives anything of genuine value from spyware or adware. Some vendors claim their software is useful, e.g. letting a user "participate in a market research community" or "access premium content." But these claims rarely survive scrutiny. For example, it is hard to see a *benefit* in being tracked for market research, when standard practice is to *pay* participants to allow their behavior to be tracked. Moreover, when a vendor promises "premium content" in exchange for popups, it turns out the supposed premium material is often readily available elsewhere for free, and/or material the vendor lacks proper license to redistribute.[4]

The harms caused by spyware and adware fall within the general realm of anti-consumer practices addressed by decades of consumer protection law. For example, just as other industries resorted to fine print to hide the unsavory aspects of their products,[5] so too do adware vendors often turn to lengthy texts, scroll boxes, or euphemisms to "disclose" key effects of their software.[6] Similarly, just as door-to-door salesmen made misleading claims to get consumers to let them in – literally, to "get a foot in the door"[7] – so too do adware vendors

---

[1] See e.g. "Who Profits from Security Holes?" http://www.benedelman.org/news/111804-1.html.
See also "Nonconsensual 180 Installations Continue..." http://www.benedelman.org/news/022006-1.html.
See also "Spyware Installation Methods." http://www.benedelman.org/spyware/installations/.

[2] "Spyware Showing Unrequested Sexually-Explicit Images." http://www.benedelman.org/news/062206-1.html.

[3] See e.g. "Zango Practices Violating Zango's Recent Settlement with the FTC" (heading "Zango Ads for Bogus Sites that Attempt to Defraud Users"). http://www.benedelman.org/spyware/zango-violations/.

[4] See e.g. "Debunking Zango's 'Content Economy.'" http://www.benedelman.org/news/052808-1.html

[5] See e.g. *Häagen-Dazs Co.*, 119 F.T.C. 762 (1995) (challenging effectiveness of fine-print footnote modifying "98% fat free" claim for frozen yogurt products that were not low in fat).

[6] See e.g. "Gator's EULA Gone Bad." http://www.benedelman.org/news/112904-1.html.

[7] See e.g. *Encyclopedia Britannica*, 87 F.T.C. 421 (1976), aff'd, 605 P.2d 964 (7th Cir. 1979), cert. denied, 445 U.S. 934 (1980) (rejecting "deceptive door opener" sales pitches).

invoke deceptive campaigns to try to attract interest in their products.[8] That the truth is (in some way) made known prior to purchase (or installation) is no defense: Once a vendor has resorted to deception, caselaw indicates that the deception cannot be cured through a (supposed) corrective disclosure. Legislation ought to consider these myriad deceptive practices – including anticipating that practices will continue to change as tricksters find new ways to deceive unsuspecting users.

The Deeper Problem: Imposing Negative Externalities on Others

In my view, spyware and adware legislation should also consider the substantial negative externalities that such programs impose on others.

For example, spyware and adware impose large costs on ISPs, computer makers, and software developers. In practice, users often turn to their ISPs and/or computer makers for assistance with problems caused by spyware and adware. Meanwhile, independent software makers must consider how their software interacts with spyware or adware unexpectedly on a user's computer – adding additional complexity and unpredictability.

Spyware and adware cause further harm to the Internet's infrastructure and to Internet users generally – even users who are not themselves infected with spyware or adware. As much as half of spam now comes from "zombie" infections.[9] Even if you keep your computer clean, others may not – and their computers may be used to send you spam.

Furthermore, spyware and adware often attempt to defraud online advertisers – typically by claiming to show ads that were never actually shown, or by showing ads that users never agreed to receive. My research has uncovered spyware and adware performing click fraud – automatically activating pay-per-click advertisement links where advertisers are only supposed to pay if a user specifically and intentionally clicks such links.[10] Spyware and adware even interfere with advertising strategies widely perceived to present a lower risk of fraud. For example, some advertisers pay advertising commissions only upon a user's purchase – protecting against click fraud.[11] But pay-per-purchase advertisers can nonetheless be tricked by spyware and adware. For example, spyware and adware popups sometimes claim commissions on purchases they actually did nothing to facilitate.[12]

In short, spyware and adware make the Internet a place where ISPs and computer makers incur unexpected costs they must ultimately pass back to customers; where even those who keep their computers safe nonetheless suffer from the infections that plague others; where advertisers cannot feel confident in the leads they pay to receive. The resulting costs make the Internet a weaker platform on which to do business, to all our detriment.

---

[8] See e.g. "Zango Practices Violating Zango's Recent Settlement with the FTC" (heading "Widespread Zango Banner-Based Installations without Unavoidable, Prominent Disclosure of Material Terms (XP SP2)") (supra).
[9] Xie et al. "How Dynamic Are IP Addresses?" http://research.microsoft.com/projects/sgps/sigcomm2007.pdf.
[10] "The Spyware – Click-Fraud Connection." http://www.benedelman.org/news/040406-1.html.
[11] These pay-per-purchase advertising systems are also known as cost-per-acquisition or "CPA."
[12] See e.g. "Spyware Still Cheating Merchants ..." http://www.benedelman.org/news/052107-1.html.

How to Stop the Problems of Spyware and Adware

Unlike the viruses of prior decades, spyware and adware tend to be created by business enterprises – groups that design this unwanted software, foist it onto users' computers, and reap the rewards. The appropriate response: Find the perpetrators and hold them accountable.

The past four years have brought considerable progress in identifying spyware and adware purveyors, and holding them accountable for what they have done. The New York Attorney General's office brought the first major case against a spyware vendor, Intermix, whose KeenValue, IncrediFind, and other programs were widely installed on users' computers without any consent at all, and also without meaningful, informed consent. Subsequent litigation has pursued a variety of other vendors, with cases brought by the FTC, the City of Los Angeles, and Attorneys General in New York, South Carolina, Texas, and Washington. Several class actions have also challenged nonconsensual and deceptive installations.[13]

The prospect of similar litigation has pushed some spyware and adware vendors to substantially cease operations. For example, in the face of litigation against several of its competitors, Manhattan-based eXact Advertising shut its "adware" business, thereby ceasing the nonconsensual installation of its software that had previously been so prevalent.

Yet litigation has not stopped the deceptive practices of all vendors. Consider the actions of Bellevue, Washington-based Zango, Inc. During an FTC investigation of its practices, Zango stopped its partners from placing its software on users' computers without first obtaining user consent. But despite its settlement with the FTC, Zango continues installations that are predicated on deception. For example, Zango continues to solicit installations via fake-user-interface banner advertisements which deceptively masquerade as bona fide messages from software already on a user's computer.[14] Moreover, despite a settlement requirement that every Zango advertisement be "clearly and prominently" identified with the name of the program that delivered that ad, some Zango advertising toolbars still lack the required label.[15]

More generally, experience and economic intuition confirm the need for *tough* litigation to adequately deter sophisticated corporate wrongdoers. At present, FTC actions typically seek disgorgement of ill-gotten gains. But effective deterrence requires a penalty that *exceeds* disgorgement, since investigation and litigation are less than certain. (Otherwise, a rational perpetrator would proceed in expectation of sometimes getting to keep the proceeds.) Experience shows inadequate deterrence to be a real problem. Consider the FTC's $1.5 million settlement with Direct Revenue – letting the company's principals retain $20 million of ill-gotten gains. As FTC Commissioner Leibowitz pointed out in his dissent to that settlement, spyware purveyors ought not reap windfalls from their deceit. To that end, I support the bill's granting of a fine of three times the amount otherwise available. (Sec. 7(b)(1).)

---

[13] See e.g. Sotelo v. DirectRevenue LLC, No. 05 C 2562 (N.D. Ill. Aug. 29, 2005).

[14] See e.g. "Zango Practices Violating…" (heading "Widespread Zango Banner-Based Installations without Unavoidable, Prominent Disclosure of Material Terms (XP SP2)") (supra). More recent (May 2008) proof on file.

[15] See e.g. "Zango Practices Violating Zango's Recent Settlement with the FTC" (heading "Unlabeled Ads – Toolbars, Desktop Icons, and Pop-Ups"). http://www.benedelman.org/spyware/zango-violations/. May 2008 proof on file.

Increasingly, purveyors of spyware and adware are not major US companies that investigators can easily locate. Instead, surviving vendors tend to reside abroad, or at least tend to attempt to hide their true location. Despite their far-flung location, these vendors sometimes cause even more harm than American counterparts – seemingly taking greater liberties with users' computers on the view that they are beyond prosecutorial reach. Legislation ought to seek to disrupt these businesses and limit the harm they cause. In my view, the most promising approach comes through financial investigations: Although they're off-shore, these vendors still want to make money, and their primary revenue sources remain US advertisers and ad networks. The New York Attorney General has already pursued selected advertisers that intentionally purchased large amounts of "adware" advertising.[16] It would be little stretch to pursue advertisers and ad networks that intentionally fund remaining spyware vendors.

Specific Concerns in the Legislation at Hand

Let me now turn to S.1625, my specific suggestions, and some areas of concern.

S.1625 Risks Setting Low Standards that Do Little to Protect Against Remaining "Adware"

S.1625 rightly prohibits a range of outrageous and extreme behaviors. For example, it would be hard to defend the "endless loop popups" prohibited by Sec. 3(1)(D).

But it is possible to skirt the bill's prohibitions while causing consumers substantial harm and continuing the same practices traditionally associated with spyware and adware. Rather than showing so many popups that a user "cannot close the advertisements without turning off the computer" (Sec. 3(1)(D)), a program might show one popup per minute – still a substantial intrusion, yet nowhere proscribed by S.1625 as it stands. Similarly, rather than tracking the specific information prohibited under Sec. 4(a), a program might monitor "only" a user's name, street address, phone number, and all web searches conducted. Although remarkably intrusive, such tracking is seemingly permitted under Sec. 4. Thus, S.1625's approach creates a serious risk that spyware and adware vendors can continue business substantially as usual.

Moreover, spyware and adware vendors are likely to attempt to use any federal legislation as a "shield" to deflect criticism of their practices. Indeed, Zango already invokes its settlement with the FTC as a supposed indicator of endorsement. Last year, Zango staff wrote to security vendors to say Zango has received "certification with the FTC."[17] More recently, Zango claimed that security vendors ought not block or remove Zango software because if Zango's software were harmful, "the FTC would not have entered into a consent agreement permitting Zango to market that software."[18] Far from setting a minimum standard that vendors will aspire to exceed, this bill thus risks creating a new supposed "certification" (or other low standard) that vendors may invoke as a defense against allegations of impropriety. As a result, weak legislation could actually make the spyware and adware problem *worse*.

---

[16] Assurances of Discontinuance – Cingular, Priceline, Travelocity. http://www.oag.state.ny.us/press/2007/jan/adware-scannedAODs.pdf.

[17] Forwarded email on file in my possession.

[18] Reply Brief of Appellant. *Zango, v. Kaspersky Lab.* US Court of Appeals for the Ninth Circuit. No. 07-35800.

Prohibiting the full spectrum of deceptive adware would require substantial reworking of S.1625. Rather than prohibiting a lengthy list of specific bad acts, a rewrite would probably begin with basic consumer protection fundamentals, e.g. that software must only be installed on a user's computer after clear and prominent disclosure as well as meaningful consent.

If S.1625 is to retain its present approach, a partially-responsive revision would add a preface or other comment to explicitly confirm the Committee's intention – that compliance with S.1625, in and of itself, does not assure that software is ethical, effective, desirable, or even useful. I realize that such an addition may seem vacuous – for of course the bill does not aspire to define what software is desirable or useful. But as the bill stands, adware vendors are virtually certain to attempt to invoke S.1625 defensively – claiming that their software must be desirable since it meets the bill's requirements. An appropriate preface could prevent that unwelcome strategy.

S.1625 Should Protect Security Vendors Assisting Users

Security vendors face a barrage of complaints and, in some instances, litigation claiming that security firms err in removing harmful or deceptive software from users' computers. See e.g. *Zango, Inc. v. Kaspersky Lab, Inc.* and *New.net v. Lavasoft*. Federal anti-spyware legislation offers a natural context in which to grant Good Samaritan protection to computer security software – immunizing the efforts of bona fide security vendors, in the ordinary course of business, to identify, block, and/or remove software users reasonably view as objectionable. S.1625 could and should include such an immunization.

S.1625 Should Not Preempt Tougher State Laws

As it stands, S.1625 preempts tougher state laws. Given S. 1625's limited prohibitions – a list of some specific bad acts, rather than a comprehensive framework for effective notice and consent – such preemption seems unwarranted.

In particular, S.1625 leaves ample room for states to do more to protect their consumers. For example, states could identify additional specific bad acts that ought not be permitted. Alternatively, states could identify alternative methods of enforcement – perhaps private litigation by those who are harmed (be they consumers, web sites, computer makers, advertisers, ad networks, or otherwise). With so much room for innovation to further address these important problems, I see no proper basis for preemption of state legislation.

A Simplified Bill Could Increase Penalties while Avoiding Other Questions

A simplification of S.1625 would strike all language except authorization of increased penalties. The treble fine in Sec. 7(b) would apply to all FTC actions under existing legislation, pertaining to software installed on a user's computer that tracks user characteristics or activities, or that shows advertising. This dramatic simplification would relieve the Committee from the challenging questions of what specific behaviors to prohibit, and would side-step all the concerns identified in my testimony. Yet this revision would offer major benefits – letting the FTC better sanction and deter perpetrators. I urge the Committee to consider this approach.