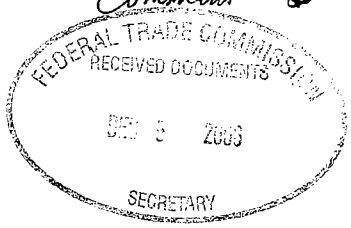
Software & Information
Industry Association
1090 Vermont Ave. NW Sixth Floor
Washington, DC 20005-4095

ORIGINAL

SIIA

Comment - 5




**Comments of the**

**Software & Information Industry Association (SIIA)**

**on**

**In the Matter of Zango, Inc., formerly known as 180solutions, Inc., Keith Smith, and Daniel Todd, File No. 052 3130**

On behalf of the members of the Software & Information Industry Association ("SIIA"), we submit our comments on the above-referenced Proposed Consent Order ("Order"), as requested in the Federal Trade Commission's ("FTC") Federal Register Notice ("Notice").[1]

As the principal trade association of the software and information content industry, the more than 800 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

SIIA has appreciated the careful and thoughtful overall approach of the FTC as it undertook to examine, investigate and reach decisions involving so-called "spyware." Beginning with a series of workshops and hearings, the FTC has appropriately sought to understand the online marketplace and its information practices, to assess the impact of these practices on consumers, and to challenge industry leaders to develop and implement meaningful self-regulatory programs.[2] The FTC has undertaken enforcement actions to fight spyware, and initiated at least six law enforcement actions that successfully challenged the distribution of spyware alleged to cause injury to consumers in the online marketplace[3] based on a realistic implementation of existing FTC authority to challenge unfair or deceptive acts and practices.[4]

---

[1] 71 Federal Register 65822-65824 (November 9, 2006).

[2] *See, e.g., Workshop: Technologies for Protecting Personal Information, The Consumer Experience* (May 14, 2003); *Workshop: Technologies for Protecting Personal Information, The Business Experience* (June 4, 2003); *Consumer Information Security Workshop* (May 20, 2002).

[3] *See FTC v. Enternet Media, Inc.,* CV05-7777CAS, (C.D. Cal., filed Nov. 1, 2005); *FTC v. Odysseus Marketing, Inc.,* No. 05-CV-330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com, Inc.,* FTC File No. 042 3196 (filed Sept. 12, 2005), available at

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

In this particular matter, SIIA has carefully reviewed the bases of this particular FTC action in light of these preceding cases, and its articulation of the larger goals and principles that it has sought to achieve.[5]

Without prejudice to the final outcome of this proceeding, SIIA is concerned that the FTC's Order and related Complaint[6] include several elements that may unintentionally create confusion for legitimate vendors of software and information products, and, if carried to their logical conclusion, may ultimately deprive consumers of tangible benefits. For a variety of reasons, SIIA urges the FTC to carefully consider how broadly to use this case as a platform for further cases involving spyware and adware.

In particular, the Complaint appears to blur the key issues of knowledge and consent, monitoring of usage, and harm to the consumer that in prior FTC cases were examined in a more integrated way. The result is that the FTC has potentially made it difficult to distinguish the alleged deceptive and unfair practices at the heart of this Complaint with the common place, appropriate actions of legitimate software companies.

In our view, prior FTC actions more typically took into account the totality of the factual situation and legal framework, alleging, for example, that a spyware distributor "used 'drive-by' tactics to install their software, which, among other things, hijacked consumers' home pages, caused the display of an incessant stream of pop-up ads, allowed the secret installation of additional software programs, and caused computers to severely slow down or crash."[7] Similarly, the FTC's prior actions have focused on how software downloads were designed into "dup[ing] consumers into downloading and installing their exploitive software code by disguising it as innocuous, free software or 'freeware'...."[8]

---

http://ftc.gov/os/caselist/0423196/0423196.htm; *FTC v. Trustsoft, Inc.,* Civ. No. H 05 1905 (S.D. Tex May 31, 2005); *FTC v. MaxTheater, Inc.,* File No.: 05-CV-0069 (E.D. Wash. Mar. 8, 2005); *FTC v. Seismic Entertainment, Inc.,* No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

[4] 15 U.S.C. § 45.

[5] See, generally, Remarks of Deborah Platt Majoras, Chairman, Federal Trade Commission, Anti-Spyware CoalitionFebruary 9, 2006, , found at: http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf; Remarks of Lydia B. Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission, the 16th Annual Conference on Computers, Freedom and Privacy, May 4, 2006, found at: http://www.ftc.gov/speeches/parnes/060504ParnesComputersFreedomandPrivacy.pdf.

[6] The Complaint is incorporated by reference into the Order. See para. 6 [sic] on p. 1.

[7] Remarks of Deborah Platt Majoras, Chairman, Federal Trade Commission before the Anti-Spyware Coalition, February 9, 2006, p. 5.

[8] Ibid at pg. 6.

In the present case, the treatment of the issues of knowledge\consent and monitoring come precariously close to independent causes of action.[9] If so, this would be a dramatic departure from FTC precedent and prior actions. As the FTC has noted elsewhere, "because monitoring software and non-monitoring software can cause harm to consumers, spyware should be defined [as such] *regardless* of whether it performs a monitoring function."[10] In this particular case, the FTC does not allege that the adware monitored use of personally identifiable information (PII), but monitored "internet use" and displayed pop-up ads based on this information.[11] Yet, monitoring Internet usage is essential to "software that many users depends upon for a safe Internet experience," including "parent control software" and "security programs that banks and financial institutions use to monitor and protect access to their online services"[12] – all of which are vital to and benefit consumers.[13]

Adding to the confusion is the treatment of the "bundled" software in the Complaint, and the treatment of so-called "lureware" (a term that is unfamiliar to our industry) as the basis for finding an alleged violation of the FTC Act. Paragraph 14 of the Complaint lists a variety of the practices that appear

---

[9] Para 16.

[10] "Staff Report: Monitoring Software on Your PC: Spyware, Adware, and Other Software", March 2005, p. 4 (emphasis added). Report is found at: http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf (hereinafter referred to as "Staff Report").

[11] See para 6 of the Complaint.

[12] Staff Report, p. 4

[13] E.g., H.R. 29 (the Securely Protect Yourself Against Cyber Trespass Act' or the `Spy Act', which passed the House of Representatives on May 23, 2005, by a vote of 393-4), after discussions with consumers, software application developers and experts, identified a number of other example of where monitoring usage was vital to and benefited consumers. Section 5(b) included the following section relevant to monitoring:

> Nothing in this Act shall apply to--
>
> (1) any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service, to the extent that such monitoring or interaction is for network or computer security purposes, diagnostics, technical support, or repair, or for the detection or prevention of fraudulent activities; or
>
> (2) a discrete interaction with a protected computer by a provider of computer software solely to determine whether the user of the computer is authorized to use such software, that occurs upon--
>
> (A) initialization of the software; or
>
> (B) an affirmative request by the owner or authorized user for an update of, addition to, or technical service for, the software.

consistent with prior findings of the FTC.[14] These all appear, from the Complaint, directly to flow from the adware software, not from the bundled "lureware." [15] Instead, the FTC's Complaint emphasizes that "In *numerous* instances, Respondents ... failed to disclose, or *failed to disclose adequately*, that the lureware was bundled with Respondents' adware that would *monitor* consumers' Internet use and cause consumers to receive numerous pop-up advertisements based on such use."[16] Taken to its logical conclusion, is the FTC Complaint suggesting that knowledge and consent is required each time software is bundled with another application? SIIA is not unfamiliar with the potential anti-consumer, anti-completive aspects of bundling in our industry and software vendors' products.[17] But, without a reading of all the fundamental issues together – knowledge\consent, monitoring, and harm – there is a distinct possibility that legitimate vendors may be lead to believe that notice and consent at each and every step of software application downloading may be required, resulting in onerous and ultimately multiple notices to consumers without demonstrated commensurate benefit.

In our view, the possibility of a *per se* requirement could be avoided by elaborating the three causes of action together and not as separate elements. This would be consistent with the prior cases --- and the FTC's own articulation of policy – that seeks to separate the pernicious effects of spyware and adware distribution from the legitimate, consumer enhancing applications that can often use the same mechanisms and techniques but which result in diametrically different results for consumers: one harmful, the other beneficial.

A second concern is with the rhetoric on End Use License Agreements (EULAs) found in the Complaint and Order. There are several places where the

---

[14] E.g., naming adware files processes with names resembling core systems software or applications; failing to identify adequately the name or source of the adware in pop-up ads so as to enable consumers to locate the adware on their computers; representing to consumers that the adware did not show pop-up ads, that that uninstalling the adware would not prevent the consumer from getting pop-up ads, and/or exaggerating the consequences of uninstalling the adware; providing an uninstall tool that failed to uninstall the adware; installing technology on consumers' computers to silently reinstall the adware when consumers have attempted to remove it manually.

[15] As we read the Complaint, nowhere is it alleged that the "purported[ly] free ... Internet browser upgrades, utilities, games, screensavers, peer-to-peer file sharing software and/ or entertainment content" were not, in fact, anything other than what it was represented to be.

[16] Complaint at p. 4 (emphasis added).

[17] See *United States v. Microsoft Corp.*, 253 F.3d 34, 58 (D.C. Cir. 2001) (en banc). See, also, Decision the European Commission of 24 March 2004 (COMP/C-3/37.792 Microsoft); *interim relief denied,* Order of the President of the Court of First Instance of the European Communities in *Case T-201/04 R, Microsoft Corporation against The Commission of the European Communities* (December 22, 2004)

Complaint,[18] and the accompanying order proscribing the Respondent from "... install[ing or download[ing] *any* software program or application without express consent",[19] is overbroad and beyond the current contours of what the FTC has required to be "clear and conspicuous." By way of example, it appears that the fact that mere "information" is found in the EULAs is an element of the Complaint. This broad brush analysis is potentially very problematic. We caution the FTC in reading this case as a basis for finding that EULA's are subject to general scrutiny, when other evidence is before the FTC that EULAs, and standardizaed licenses generally, have broad-based benefits to consumers and the economy generally.[20]

Finally, in contrast to many of the prior actions by the FTC in this area, the Complaint includes merely summary or cursory facts regarding the technology and business methods used by Zango. This makes it difficult to assess with confidence what, in fact, was the predictable basis for the FTC's actions. In this area, where the FTC has recognized that "fundamental issues remain to be resolved before a clear and definitive definition of spyware" can emerge, with particular emphasis on the "fundamental issues of consent and harm [that] need to be resolved before any common definition of spyware can be developed",[21] a complete establishment of the facts at issue is essential.

SIIA appreciates this opportunity to comment on this Order. Please do not hesitate to contact Mark Bohannon, General Counsel & SVP Public Policy at SIIA (mbohanon@siia.net) if we can answer any questions or provide additional information.

---

[18] "In some instances, ... *information regarding* Respondents' adware was available only ... in lengthy terms and conditions regarding the lureware." Complaint at p. 2, para. 11.

[19] Order at p. 5, Section III.

[20] See, e.g., **Warranty Protection for High-Tech Products and Services,** FTC Symposium held on October 26-27, 2000, found at: http://www.ftc.gov/bcp/workshops/warranty/index.html.

[21] Staff Report, pg4,5. We note that the Complaint includes a new term, "lureware", which heretofore has not been used by the FTC, nor is it familiar to our industry.