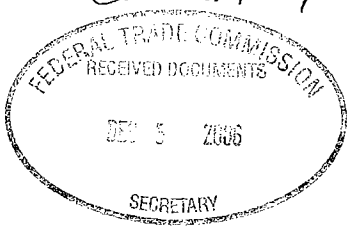
ORIGINAL

Comment - 4



DMA
Direct Marketing Association

December 5, 2006

Via Electronic Filing

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room 135-H
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Zango, Inc., File No. 052 3130

Dear Secretary Clark:

The Direct Marketing Association ("DMA") appreciates the opportunity to submit these comments in response to the Federal Trade Commission's ("FTC" or "Commission") request for public comment on its proposed consent agreement with Zango, Inc., 71 Fed. Reg. 65822-65824 (November 9, 2006).

DMA is the largest trade association for businesses interested in direct, database, and interactive marketing and electronic commerce. DMA represents more than 4,000 companies in the United States and 53 other nations. Founded in 1917, its members include direct mailers and direct marketers from 50 different industry segments, as well as the non-profit sector. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

DMA member companies have a major stake in the success of electronic commerce and Internet marketing and advertising, and are among those benefiting from its growth. As described more fully below, DMA has been active in developing and adopting guidelines and best practices for our members in connection with software and other technology downloads on computer and similar devices.

DMA appreciates the important role that the Commission has played in combating deceptive practices in connection with software downloads, and in targeting bad actors and practices, such as surreptitious surveillance, modem hijacking, or other programs that take over and ruin computers. In addition, we recognize the important contributions that the Commission has made in furthering the dialogue on these issues and in educating consumers and businesses alike through its numerous workshops, publications, and other online resources on these issues.

DMA's comments herein are focused on the issue of express consent for software and other application downloads. In Part III of the Proposed Consent Order, the Commission prohibits Respondents from, or assisting others in, installing or downloading any software program or application onto any computer without express consent. "Express consent" is defined in the proposed order to require (1) clear and prominent disclosure of material terms prior to and separate from any Final End User License Agreement, and (2) consumer activation of the download or installation via clicking a button or a substantially similar action. (*See* Agreement Containing Consent Order, Page 5 of 12)

Although this type of approach may be appropriate in this situation, consent separate from an End User License Agreement (EULA) is not a standard that would be appropriate for many software downloads.[1] First, requiring separate consent in many instances could undermine the consumer experience at many Web sites, as well as inhibit the overall growth and success of e-commerce. Separate consents would have the effect of considerably slowing the consumer's experience in a manner that consumers would resist. They also would limit the innovative and seamless behind-the-scenes technologies that allow for personalization and customization of Web sites and Internet experience that consumers desire.

With this type of approach, consumers would be inundated with "pop-up" and multiple other notices which, ironically, could have the effect of undermining the value of the notice and informed consent; a significant increase in notices likely would cause consumers to disregard them altogether and become frustrated with the associated delays. This is particularly true given that the term "software" is not defined in the proposed consent order. In addition, a requirement of notice separate from the EULA would burden businesses by requiring them to provide and keep track of numerous notices, and would be cumbersome to implement.

Moreover, acceptance of EULAs through so-called "click-wrap" licenses is commonly used in connection with e-business transactions, and there is significant legal precedent regarding their validity and enforceability in electronic contracting. *See, e.g., ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) and its progeny, including *Hill v. Gateway,* 105 F. 3d 1147 (7th Cir. 1997) (upholding shrink-wrap licenses—the predecessor to click-wrap license), *Hotmail Corp. v. Van$ Money Pie Inc.,* 1998 WL 388389, 47 U.S.P.Q.2d 1020 (N.D.Cal. Apr 16, 1998), *Moore v. Microsoft Corp.*, 741 N.Y.S.2d 91 (2002). It is important that this long-standing precedent be recognized and

[1] As the Commission has noted in response to comments on other proposed consent agreements, in cases against alleged wrongdoers, measures above and beyond legal requirements may be warranted as "fencing in relief." *See, e.g.,* FTC March 7, 2006 letter to Visa in re: DSW Inc. Matter No. 0523096, p. 1 n. 1 (re: fencing-in remedies and their breadth in scope beyond the conduct that is declared unlawful in a particular case), http://www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterVisa.pdf.

given full effect. Again, the lack of clearly defined terms with respect to what constitutes software makes an approach of separate consent particularly troublesome.

Thus, DMA believes that the framework that the FTC is proposing to address the specific conduct and software downloads at issue should not have broader application for all software and application installations, irrespective of intended uses and how these technologies collect data. In addition to the practical and legal points raised above, also of note is that DMA and other industry group have worked extensively to develop appropriate standards and guidelines regarding various types of software downloads, focusing on how the technology is used, rather than adopting a blanket rule requiring a specified consent for all software or applications.[2] (*See* Exhibit One below—Article 40 of DMA's Guidelines for Ethical Business Practice entitled *Use of Software or Other Similar Technology Installed on a Computer or Similar Device; see also* TRUSTe's Trusted Download Program, which is available at http://www.truste.org/trusteddownload.php.)

These guidelines also distinguish between cookies and other similar technologies, recognizing that other means of notice and/or consent are appropriate in the context of these types activities. In addition, DMA and other industry guidelines and best practices focus on notice and choice before the software begins operating (or at the point of joining a service), or affirmative consent beforehand.

In conclusion, DMA believes that the requirements of Part III of the proposed consent agreement should remain focused on the specific conduct at issue in this settlement, and not have a broader future impact on all software downloads. DMA wishes to underscore the importance of ensuring continued consumer benefits and viability of online advertising, and the careful balance that is reflected in current industry guidelines and best practices. It also is important to refrain from inhibiting the functioning of innovative and seamless technologies that are integral to a positive online experience and to long-standing law regarding electronic contracting, which is important to the continued growth of e-commerce.

* * *

DMA appreciates the opportunity to comment on the proposed consent order and highlight some of the broader issues and industry best practices related to software

---

[2] Chairman Majoras recently remarked at the Commission's Public Hearings on Protecting Consumers in the Next Tech-ade that "consumer protection concerns that technological advances create often can be addressed without the passage of new laws or the issuance of new regulations." *See* http://www.ftc.gov/speeches/majoras/061106dpmtech-aderemarksltrhd.pdf. This is particularly true where rapidly evolving technology is at issue as is the case with software downloads.

downloads. For additional information, please call me at 202/955-5030 or Stuart Ingis, Venable LLP, at 202/344-4613.

Sincerely,

Jerry Cerasale
Senior Vice President, Government Affairs

cc: Stuart Ingis, Venable LLP
Alisa Bergman, Venable LLP

Attachment

DMA
Direct Marketing Association

Exhibit 1

Excerpt from DMA Guidelines for Ethical Business Practice

Use of Software or Other Similar Technology Installed on a Computer or Similar Device

Article #40

Marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include, but are not limited to, software or other similar technology that:

- Takes control of a computer (e.g., relaying spam and viruses, modem hijacking, denial of service attacks, or endless loop pop-up advertisements)
- Deceptively modifies or deceptively disables security or browser settings or
- Prevents the user's efforts to disable or uninstall the software or other similar technology

Anyone that offers software or other similar technology that is installed on a computer or similar device for marketing purposes should:

- Give the computer user clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects* of having the software or other similar technology installed
- Give the user an easy means to uninstall the software or other similar technology and/or disable all functionality
- Give an easily accessible link to your privacy policy and
- Give clear identification of the software or other similar technology's name and company information, and the ability for the user to contact that company

* Determination of whether there are significant effects includes, for example:

- Whether pop-up advertisements appear that are unexpected by the consumer
- Whether there are changes to the computer's home page or tool bar
- Whether there are any changes to settings in security software, such as a firewall, to permit the software to communicate with the marketer or the company deploying the software, or
- Whether there are any other operational results that would inhibit the user's expected functionality

Cookies or other passive means of data collection, including Web beacons, are not governed by this Guideline. Article #37 provides guidance regarding cookies and other passive means of data collection.

Comment:

- DMA's Board of Directors approved this guideline (in January 2006) in order to assist members in defining minimally acceptable marketing practices in the area of software installation practices. (The Board also approved a six-month phase-in period to allow for any programming changes companies may need to make for implementation.)

- Software by itself is neutral, and the use of software and other similar technology to assist consumers is beneficial. This guideline supports DMA's vigorous opposition to the fraudulent, deceptive or unscrupulous use of software or other similar technology to harm the interests of consumers. The guideline's focus, therefore, is to prohibit practices that are deceptive. (Not all possible deceptive practices are listed, as new ones will, unfortunately, be implemented by unscrupulous operators in the future.) Controlling a user's computer and preventing users from uninstalling unwanted software are examples of deceptive or harmful practices.

- The guideline does not use terminology such as "spyware" or "adware." It was decided that the terminology used should be neutral and broad (e.g., "software and other similar technology") because of the continuous evolution of online technology. ("Spyware" or "malware" generally refer to software that has negative consequences for computer users, while "adware" generally refers to software that places legitimate advertisements.)

- Federal and state legislators are extremely concerned about the negative consequences of "spyware," or applications that harm users' computers in various ways, and have introduced numerous legislative bills. DMA ethics guidelines are meant to get "ahead of the regulatory curve" by demonstrating effective self-regulation.

- The guideline refers to "software or other similar technology installed on a computer or similar device" because it is meant to encompass such things as PDAs and MP3 players, etc. (and future similar inventions) as well as computers.

- The guideline does not include "cookies," "Web beacons," or other such passive means of data collection. Rather, it focuses on the effects of software that is installed on computers.

- By stating: "Anyone that offers software or other similar technology that is installed on a computer...," the guideline is conveying that there is broad responsibility for

who is responsible for the software offer. Responsibility belongs to both the marketer and the service entity it may employ.

- The standard of giving computer users "notice and choice" before the software begins operating (or at the point of joining a service) is the DMA guideline. However, marketers can go beyond the basic standard if they choose, for instance, by getting users' affirmative consent beforehand.

- Marketers should not be held responsible for inactive software that may inadvertently remain on a user's computer. The guideline reads: "Give the computer user an easy means to install the software or other similar technology and/or disable all functionality" because it is difficult to assure that each and every component of an installation can be completely removed. In addition, some effects of software installation, including changes to registry settings (i.e., configuration files within Windows) may go unnoticed.

- Reference to the "significant effects" of having software installed is not meant to be all-inclusive because new applications are always emerging.

- It is essential that marketers make sure they provide an easily accessible link to their privacy policy so that computer users can review what information may be collected as a result of the software installation, and how it may be used. Such transparency serves to encourage consumer trust in your company.

Questions to Ask:

- Have you assessed whether any programming changes are needed for implementation of the guideline, and made such changes?

- Have you reviewed your online privacy policy to make sure it appropriately covers significant effects, as outlined, of software installations?

- Is notice and choice provided to computer users easy to find, easy to read, easy to understand and easy to act upon?

- Have you been sure to identify the software being installed, as well as your company name and information, in case the computer user wants to contact you?

- Have you given users an easy means to uninstall and disable the computer software?

Best Practices

Marketers should get users' affirmative consent before computer software is installed and/or begins operating.

Marketers should help users in not only uninstalling software, but making sure users' computers are returned to their original settings (prior to software having been installed).