

November 18, 1999



WEB BUGS: TEN STEPS YOU SHOULD TAKE

Internet advertisers are collecting detailed information about the online behavior of consumers. Consumers may not be aware this is happening. Web site operators need to notify consumers of the information collection practices associated with their pages (whether these practices are controlled by third-party advertisers or the web site itself) and give consumers a reasonably-accessible method for opting out.

What's a web bug? A web bug (sometimes called a "clear gif" by the advertising industry) is an inconspicuous graphic loaded on a web page, usually from a different server than that used for the rest of the page. Web bugs are often invisible because they are extremely small. They are placed on a page to allow the source to record "hit" information about visitors to that page. (A "hit" is the retrieval of any item, like a page or a graphic, from a web server.) This hit information is reported to the advertising networks who have a relationship with the site.

What information does a web bug report? A web bug gathers the Internet Protocol (IP) address of the computer that produced the hit. (An IP address is the unique numeric identifier for a computer attached to the Internet.) It also reports

the Universal Resource Locator (URL) of the page on which the web bug was placed (e.g., www.quicken.com); the URL for the web bug graphic or image (which usually comes from a different server); the time the web bug was viewed; the kind of browser (e.g., Internet Explorer) the user is using; and information about any "cookie" set by the web bug. (A "cookie" is a piece of information stored on the user's disk drive when the web browser accesses a server. The browser stores the information in a text file, and this information is sent back to the particular server each time the browser retrieves a page from that server. Cookies are used to identify unique users.)

Because each advertising company has relationships with a network of sites, information gathered from multiple web bugs hit by a single user can help the advertising network build a detailed profile of what sites a particular person is visiting, and their activities on those sites.

Why should you care? On November 8, the Department of Commerce and the Federal Trade Commission held a joint public meeting on online profiling — the creation of numeric profiles of users' online activity by advertising agencies and others. At this meeting, representatives of the Internet advertising industry and consumer groups discussed advertisers' practice of placing "web

bugs” that collect information about users’ activity on a particular site. Consumer groups expressed strong opposition to this practice.

During the afternoon portion of the meeting, a group of Internet advertising networks (24/7 Media, AdForce, AdKnowledge, Adsmart, DoubleClick, Engage, Flycast, Matchlogic, and RealMedia) announced the formation of a self-regulatory group called the Network Advertising Initiative (www.networkadvertising.org). These companies have agreed to provide notice to consumers of their profiling practices; to provide an easy-to-use opt out method; to educate users about profiling (through their web site); to require publishers to provide a link to their disclosure statements about their practices; and (eventually) to agree to a third-party audit to enforce these agreements. The Network Advertising Initiative has promised that users will be able to opt out of all use of personally-identifiable information. Additionally, users will be able to opt out of all collection of advertisement delivery data concerning them — but users won’t be able to opt out of the collection of aggregate “reach” data (data on the overall numbers of users viewing particular advertisements), which the companies termed essential to the “infrastructure” of the Internet.

The Federal Trade Commission has announced that it intends to examine the impact of web bugs on consumer privacy.

What’s the problem? Consumers don’t know about web bugs or online profiling. Many people feel very uncomfortable once they learn that their actions are being closely monitored. If a consumer curious about web bugs looks at a site’s privacy policy, the policy will likely say nothing about what third-party advertising networks are doing through the site. This could lead to claims that many privacy policies, drafted with a view to the practices of the web site owner (not the entire network of sites using an ad placement service) are misleading.

Ten things operators of web sites can do:

1. Find out what the advertising networks are learning about your visitors. (Consider whether advertisers’ access to information about visits to particular pages on your site might be viewed as especially sensitive.)
2. Make sure that your privacy policy clearly discloses to visitors what information is being gathered about them by advertising networks through your site.
3. Provide a link in your privacy policy to the disclosures of the advertising networks placing web bugs on your pages.
4. Educate yourself about the opt-out options being provided to your visitors by the advertising networks with whom you have relationships.
5. Make sure that your privacy policy clearly discloses to visitors how they can opt out of the collection of information about them by the advertising networks.
6. Consider eliminating the use of non-advertising, invisible web bugs on your pages (web bugs that are not associated with actual advertising on which users affirmatively click).
7. Educate yourself about the access your visitors will be provided to the profiles being built about them by the advertising networks.
8. Find out whether your visitors will be allowed to erase inaccurate information about themselves from online profiles.
9. Make sure that your privacy policy clearly discloses to visitors what access they will have to the online profile information prepared about them by the advertising networks.
10. Ensure that any advertising network with whom you have a contractual relationship has agreed to be part of a self-regulatory program

agreed to be part of a self-regulatory program (like the Network Advertising Initiative) and a third-party seal program (like bbbOnline or TrustE) that will enforce their privacy promises.

David R. Johnson djohnson@wilmer.com,
202/663-6868

Susan P. Crawford scrawford@wilmer.com,
202/663-6479

MONTHLY UPDATE

Access arrest overturned. A Munich court has overturned the 1998 conviction of a CompuServe executive in Germany for failing to block access to child pornography sites on the Internet.

ADA/litigation. The National Federation of the Blind, and nine individuals, all of whom are blind, sued America Online, Inc. ("AOL") on November 4th in federal district court in Boston, alleging that AOL's online service violates the Americans with Disabilities Act. The complaint alleges that AOL has denied blind Internet users access to its popular online service by employing software that is incompatible with special screen access programs that dictate text and otherwise assist blind users in navigating the Internet.

Cybersquatting. A compromise version of legislation (S. 1255) to prevent unauthorized use of proprietary brand names and personal names on the Internet has been attached to the conference report for the Satellite Home Viewer Act (H.R. 1554). House and Senate leaders are currently negotiating to have the bill included in the omnibus appropriations package that is scheduled to be considered shortly by Congress.

Privacy/litigation. Seattle-based RealNetworks was recently hit with several lawsuits accusing the company of violating the privacy of millions of web music listeners. The suits allege that RealNetworks secretly collected information on customers' music choices while they were downloading selections from the company's popular RealJukeBox software. One of the actions, a

class-action lawsuit filed in California, seeks \$500 million in damages. RealNetworks has responded that it neither stored nor used any of the personal information it may have collected, and has characterized the suits as meritless.

Privacy/safe harbor. On November 15, the Department of Commerce released the latest version of discussion documents which, when finalized, will provide a basis for a "safe harbor" for U.S. entities seeking to comply with the European Union's stringent Directive on Data Protection. Under the latest Commerce draft, U.S. entities seeking safe harbor treatment must observe seven key privacy principles, including the provision of notice to consumers of data collection practices, an opportunity for consumers to "opt-out" of certain uses of their personal data, and the establishment of adequate data security and consumer enforcement mechanisms. The deadline for comments on these new documents (posted at www.ita.doc.gov/ecom) is December 3, 1999.

Y2K. On November 17, the Department of Commerce released a report on the economic impact of the Y2K computer problem. The report, entitled *The Economics of Y2K and the Impact on the United States*, examines the effects of domestic and foreign Y2K problems and preparation, including the costs of remediation; the effects on business productivity, inventories and GDP; and the impact of potential changes in consumer/market behavior. The report concludes: "Y2K problems at home and abroad should have only minor and short term effects on U.S. economic growth."

This memorandum is for general purposes only and does not represent our legal advice as to any particular set of facts, nor does this memorandum represent any undertaking to keep recipients advised as to all relevant legal developments.

E-Commerce News also available at <http://www.wilmer.com>