

# Internet Cookies, Web Bugs and Spyware

---

## *The John Marshall Law School*

**By Henry N. Meier, Jr., Esq.**  
*Of Counsel, CorpLaw Associates LLC*



Henry is Of Counsel to CorpLaw Associates LLC. He has over 20 years of experience in IP, corporate transactional, and e-commerce law. He can be reached at [henry@corplaw.com](mailto:henry@corplaw.com) or at 847.784.1300. The firm's web site is [www.corplaw.com](http://www.corplaw.com).

### 1.0 Key Terms Defined

1.1 Clickstream data. The data trail that an Internet user leaves behind while performing operations on the Internet, such as entering data into search engines and visiting Web sites.

### 1.2 Cookie

1.2.1 A benign definition. A cookie is a unique identifier that may contain a serial number, contained in a text file that a computer hosting a Web site (computer 1 or "c1") causes to be written/placed on the hard drive of a computer that requests this Web site (computer 2 or "c2"). Each time that c2 requests any page from the Web site hosted by c1 thereafter, the identifier is sent back to the Web site (c1), and serves to identify computer 2. The identifier stored in the cookie can be used to associate all clickstream data collected from c2 into a single record of file (dossier?). The computer for the Web site, c1, may use data in this file/dossier to target customized information or advertisements to the user on c2, based on inferences about the user's preferences as revealed by the clickstream data collected.

1.2.2 From advertiser's/browser's perspective. A cookie is a general mechanism which server side connections can use to both store and retrieve information on the client side of the connection. The addition of a simple, persistent, client-side state significantly extends the capabilities of the Web-based client/server applications.

1.2.3 From EPIC - Electronic Privacy Information Center. A cookie is a mechanism that allows a Web site to record the user's comings, goings and operations at the Web site, usually without the user's knowledge or consent.

1.3 Web Bugs, a/k/a Web Beacons. A Web Bug functions in a "third party" setting. The computer hosting a Web site (computer 1 or "c1") serves the site to a user's computer (computer 2 or "c2"). A Web Bug is an instruction in the HTML code of a Web page that causes the user's computer, c2, to transmit information across the Internet to some other computer (computer 3 or "c3" - or "c4", "c5", or "cX"), under the pretext of obtaining a graphic image from that other computer, c3 - cX. This image is placed on the Web page that c2 has requested for viewing. The Web Bug gathers information from user's

computer, c2, and places it in a string of text that is attached by c2's browser to its request to view the Web site. This information is sent to c3 along with the request for the image. The image that the Web Bug causes c2's browser to get generally consists of a single pixel that is the same color as that of the Web page. This pixel has no effect on c2's display, and therefore cannot be seen. In banner ads, this technology works whether or not you click on the ad itself!

- 1.4 Spyware a/k/a Adware. Spyware is hidden software code which transmits user information via the Internet to advertisers in exchange for free downloaded software. Spyware is often application based code which software developers build into their product. It could cause the user's computer to transmit information back to the software developer, such as reporting on other installed software after the user's entire hard drive is scanned. See ZDNet article, attached.
- 1.5 Other Types. Globally Unique Hardware Identifiers - related to Ethernet cards on a LAN, and Email and document bugs - to see subsequent string of Email messages.
- 2.0 Background Information
- 2.1 Data Collected. Data collected may include a user's account number, password, ID code of any cookie, credit card information or other stored information, pages viewed, user's operating system and Web browser, user's IP address, the kind of computer and software used, and other similar information.
- 2.2 Cookie and Web Bug Compared. A cookie is actually placed on the user's hard drive; Web Bug is not. Web Bug is more powerful. Cookie sends information only back to Web site server; web Bug can send to any server. Both function without any action by, and without any notice to, the computer user.
- 2.3 Legitimate Use? Advertisers claim these methods enable them to serve tailored advertising. To provide the user with a more personalized experience?
- 2.4 Users of These Technologies. Real Networks, Amazon, Microsoft, Mattel, and others.
- 3.0 The Problem. Advertisers claim that these methods do not gather personally identifiable information. Can info be combined? Information from multiple sites? Combine with personally identifiable database?
- 3.1 Privacy Issues. Most prefer to surf the Internet anonymously. This technology allows tracking of a your whereabouts, search strings and habits. Online profiling data can easily be connected with personally identifiable information.
- 3.2 Disclose Use. Since these technologies work "behind the scenes", consumers are not aware of their presence or use. They do not know which of their data is being monitored and collected, nor do they know where this data is being assembled and maintained. If unaware of online profiling activities, why should consumers be required to actively search for privacy policies and actively opt-out from these practices?

- 3.3 Who's Responsibility? Should Web site business disclose use of these technologies to consumer and how to opt-out? Does consumer have an affirmative obligation to track down the surveillance technology of each site visited, AND consent to each use?
- 4.0 The Solution
- 4.1 Zap it! Remove cookies and spyware. Many Web sites offer software solutions to identify the type of surveillance tool and remove it. See Geek Girls article.
- 4.2 Opt-Out. If the Web site offers an opt-out option, use it.
- 5.0 Actions and Activities
- 5.1 Legal Status. Few laws currently. Case law developing.
- 5.2 FTC Activities. FTC is tracking these activities as part of its Privacy initiative. FTC has reviewed activities of Doubleclick.
- 5.3 Attorney General. Michigan AG took action against web site advertisers as a violation of Consumer Protection Act. Theory: disclose use of Web Bugs.
- 5.4 Private Action. In re Doubleclick Privacy Litigation. 154 F. Supp. 2d 497 (SD NY, 2001)
- 6.0 Resources - Web Sites and More. Photocopies of some Web Sites are attached.
- 6.1 Federal Trade Commission: [www.ftc.gov](http://www.ftc.gov) .
- 6.2 [www.spychecker.com](http://www.spychecker.com) . A global database of spyware programs.
- 6.3 Electronic Privacy Information Center. [www.epic.org](http://www.epic.org) . Has a searchable database.
- 6.4 Center for Democracy and Technology. [www.cdt.org](http://www.cdt.org) . Has searchable database.
- 6.5 [www.privacy.net](http://www.privacy.net) . Has searchable database.
- 6.6 [www.cexx.org](http://www.cexx.org) . Has downloadable solutions to Zap! adware and spyware.
- 6.7 Another View: [www.networkadvertising.org](http://www.networkadvertising.org) . This is a group of network advertisers. It, too, has developed privacy principles. NAI approved DoubleClick's opt-out format.
- 6.8 INTERNET COMMERCE - The Emerging Legal Framework, Cases & Materials, foundation Press, © 2002.

*CorpLaw Associates LLC is a law firm of experienced business attorneys who deeply understand their clients' businesses and who use best practices to achieve their clients' business goals. The firm provides full support for businesses. For clients who need on-site legal help, CorpLaw is one of only a few firms that specializes in this model. Our mailing address is CorpLaw Associates LLC, 400 Central Avenue, Suite 150, Northfield, Illinois 60093. We can be contacted at 847.784.1300 or at [firm@corplaw.com](mailto:firm@corplaw.com). Our web address is [www.corplaw.com](http://www.corplaw.com).*