



200 CONNECTICUT AVENUE – 5TH FLOOR
NORWALK, CONNECTICUT 06854
203-838-8500
Facsimile: 203-854-1652
www.levberlin.com

MEMORANDUM

Privileged and Confidential

DATE: October 14, 2010

RE: Flash Cookies

In the last few months, class action lawsuits have been filed against three major Internet advertising technology providers, Quantcast, Clearspring and Specific Media, over their use of locally shared objects, colloquially known as “flash cookies.” A fourth class action lawsuit has been filed against Ringleader, a web analytics company that deployed an HTML5 application to track users’ web browsing on mobile phones. With the exception of the lawsuit against Specific Media, each lawsuit also named as defendants a number of major content providers, such as CNN and MTV, which had allowed these technologies to be placed on their websites. This newsletter provides a brief description of the technologies at issue, explains the law and theories behind these four lawsuits, and provides some general recommendations on how to lawfully and ethically use these technologies. If you are unsure if your website is using flash cookies, this would be an opportune time to evaluate whether your website uses flash cookies or some other technology, such as HTML5, and what those technologies are designed to do.

While web developers have used flash cookies since 2005, their use has become sufficiently widespread now to enter the consciousness of general web users. For example, the Wall Street Journal ran a series of stories in July on the use of flash cookies and the tracking of users’ web browsing. Like traditional HTML cookies, flash cookies are used to track users and store information about them. Unlike traditional cookies, flash cookies base their existence within Adobe’s Flash application, and offer a number of advantages (from the developer’s perspective) over HTML cookies. Flash cookies can be larger, do not expire and are not stored within a browser, and therefore are not deleted when a user chooses to delete all cookies using the browser’s privacy functions. In addition, flash cookies can be used to “re-spawn” or restore traditional HTML cookies upon their deletion. HTML5 is simply the next version of the standard web programming language, but among its new features is the enhanced ability for developers to store data on users’ devices. In this way, HTML5 “cookies” are similar to flash

cookies. This functionality has a number of benefits, such as the possibility for offline access to websites, but also allows for applications such as those in the Ringleader lawsuit to be used.

The use of flash cookies and similar technologies presents a number of legal risks, including: 1) an FTC enforcement action for unfair trade practices (Adobe has specifically asked the FTC to become involved on this subject); 2) a regulatory action in the European Union; and 3) private lawsuits, such as those mentioned earlier. The steps that are required to comply with these applicable laws and/or to avoid lawsuits depend on how the flash cookies or similar technologies are being used.

The FTC has not provided a comprehensive set of regulations or guidelines that cover the use of cookies or online privacy practices; however, the FTC has regulated in this area through civil lawsuits and has issued best practices on certain specific topics, such as with respect to behavioral advertising. Through its civil enforcement actions, the FTC has mandated that companies that post privacy policies comply with the requirements that they set for themselves. For example, the FTC investigated in 2001 whether DoubleClick conducted an unfair trade practice by proposing to combine personally-identifiable information with tracking data, despite DoubleClick's assurances in its privacy policy that all tracking information would remain anonymous. DoubleClick agreed not to combine the databases and the FTC required DoubleClick to make substantial revisions to its privacy policy.

Under the EU's Privacy and Electronic Communications Directive, consumers must be given notice about the utilization and purpose of any cookies used by a website and given the ability to withhold consent. Currently, notice may be provided through a conspicuous privacy policy and user consent can be expressed through the use, or lack thereof, of browser preferences. These regulations are in a current state of flux as regulations that may require a more express indication of consent by the user have been passed by the EU and are currently being interpreted by member states.

In the four class action lawsuits mentioned above, the plaintiffs asserted violations of a number of federal and state computer and privacy statutes as well as several common law claims, including: the federal Computer Fraud and Abuse Act and the Electronic Communications Act, the California Computer Crime Law and Invasion of Privacy Act as well as common law unjust enrichment and trespass claims. In all four lawsuits, flash cookies or a similar HTML5 application were allegedly being used to track users' browsing by assigning a unique identifier to each computer. The cookie would relay back information when the user would visit a website served by a particular advertising network using the technologies. In all four cases, many of the content providers' websites entirely failed to disclose the use by the relevant advertising network of flash cookies (or HTML5) on their websites. In addition, in each of the Quantcast, Clearspring and Specific Media lawsuits, the flash cookies were being used to re-spawn deleted cookies. The alleged violation of each statute and common law claim can ultimately be reduced to the accessing by each of the four main companies and the other

content provider defendants of the users' computers without authorization or exceeding any authorization that was given.

Ordinarily, HTML cookies are used by developers for authentication, storing site preferences, shopping cart contents or identifiers for a server-based session on a single website. Flash cookies and HTML5 can be used for the same purposes. Where flash cookies and HTML5 are being used for the same functions as traditional HTML cookies, the principles of notice and choice apply. In the context of flash cookies, which are not necessarily controlled through browser preferences, easy instructions should be given to the user on how to "opt-out" of receiving the cookie. The use of flash cookies to re-spawn/restore deleted HTML cookies is almost certainly illegal. The practice defeats the consumer's choice and thereby would violate the relevant EU laws, constitute an unfair trade practice in the US and also likely violate many of the laws cited in the four class action lawsuits.

Where HTML and flash cookies and other technologies are being used to track user web browsing across websites or computer activity in general, it is clear that the consent of the user must be obtained. The FTC filed a complaint against Sears in 2009 alleging that Sears had committed an unfair trade practice by employing a tracking application that monitored a user's entire web browsing without proper consent. In the resulting consent order with Sears, the FTC laid out the requirements for such a program. A "tracking application" is broadly defined as "any software program or application disseminated ... that is capable of being installed on consumers' computers and used ... to monitor, record or transmit information about activities occurring on computers on which it is installed..." The FTC required Sears to clearly and prominently display on a screen separate from its privacy policy a page that disclosed all types of data collected, including where such information will be collected, how the data may be used and whether the data may be used by a third party. Further, Sears was required to obtain express consent from the consumer before the application could be downloaded. The use of cookies, including flash cookies, to collect information across websites certainly would appear to fall under the umbrella of the FTC's rules in the Sears consent order.

In summary, flash cookies and other new technologies, such as HTML5, that are used to store data on users' computers and other devices, need to be clearly disclosed to the user. Where the use of the flash cookie or other technology is limited to the website deploying it, such as for authentication, then a separate disclosure in a privacy policy, including instructions on how to block or uninstall the flash cookies or other technology, should be sufficient. Where the use of the flash cookie or other technology is used to monitor activity across websites or computer use in general, under FTC jurisprudence, a separate, specific disclosure must be given to the user and explicit, up-front consent received. Under no circumstances should a flash cookie or other technology be used to restore deleted HTML cookies.