e-commercelaw&policy

FEATURED ARTICLE

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Cookies 2.0: Flash cookies, user profiling and privacy

What is a Flash cookie? Well, have you ever noticed that some websites seem to know more about you than your own spouse - for example, online retailer websites which suggest products you might be interested in based upon other products that you have purchased or even just looked at in the past, or social networking sites that offer advertisements to you based upon your previous postings or comments, and even internet-based email services that suggest searches for topics about which you just happened to have emailed your friends? How is any of this possible, you ask? Answer: Through the use of so-called 'Flash cookies', which differ from browser cookies in that they are special 'cookies' utilised by Adobe Flash software, are difficult to avoid and detect on an individual's computer, and cannot easily be blocked or deleted using the basic privacy control features offered by most internet browsers. Melinda Levitt and Yonaton Aronoff, of Foley & Lardner LLP, analyse how these 'super' cookies work and what their implications are for privacy and data security.

Flash cookies have allowed targeted online marketing to become a multi-billion dollar international industry, with online advertisers building a big business out of 'profiling' consumers by tracking their browsing and purchasing activities, and utilizing those profiles to create more effective, targeted advertisements that are uniquely tailored to a consumer's preferences. Many argue that the growth of this business has kept the internet free. Others contend that the tradeoff - less personal privacy for consumers - is far too costly and invasive, and cannot be controlled or easily eliminated via the various 'Do Not Track' and 'opt out' protections supposedly available to privacy-sensitive consumers.

Whether or not those advocating in favor of more privacy are correct, their cause certainly suffered a setback by way of the 17 August 2011 decision in Bose v Interclick, Inc.[1], a putative class case pending in the US District Court for the Southern District of New York. In Bose, the lead class Plaintiff sued Interclick Inc., an online advertising network, along with several advertisers (including McDonalds, Microsoft and Mazda), for allegedly violating the federal Computer Fraud and Abuse Act (CFAA), New York General Business Law § 349, and New York State common law. The Plaintiff contended that the Defendants used 'Flash cookies' and 'history sniffing' software code to create profiles of the plaintiff for targeted advertising, invading the Plaintiff's privacy and injuring her in the process. The complaint alleges that the Defendants caused 'Flash cookies' to become stored on the Plaintiff's computer, unbeknownst to her and that the 'history sniffing' program code tracked the Plaintiff's website visits without her knowledge or consent.

The Defendants moved to dismiss the complaint, arguing, among other things, that the Plaintiff had failed to plead sufficient allegations of economic injury as required by the CFAA. Judge Deborah A. Batts agreed with most of the Defendants' arguments, and dismissed all of the claims against the advertiser Defendants and all but two of the claims against Interclick. In dismissing the Plaintiff's CFAA claim, Judge Batts relied heavily on In re DoubleClick Inc. Privacy Litig.[2] ('DoubleClick'), which held that plaintiffs claiming injury from internet tracking software and purported privacy violations must plead quantifiable economic injury. Under the analysis in DoubleClick, Judge Batts found, the Bose Plaintiff's claims were defective in that they failed 'to make any specific allegation of damage to her computer' and that generalized claims of 'harm' due essentially to loss of privacy or the loss of 'value' of a plaintiff's personal information do not constitute cognizable economic losses under the CFAA. However, Judge Batts allowed the Plaintiff's claims under New York state's deceptive business practices statute to proceed, as well as the Plaintiff's trespass claim, but commented that these allegations were 'of dubious merit'.

In light of Bose and DoubleClick, as well as the recent decision in LaCourt v Specific Media, Inc.[3], (dismissing claims involving 'Flash cookies' for failure to plead sufficient allegations of economic injury), plaintiffs asserting privacy-invasion claims based upon unwanted 'Flash cookies' face an uphill battle in court.

With the courts deciding the federal statutory relief is not available under the CFAA, consumers must hope for regulatory relief, in particular from FTC. One might think the FTC

would have acted on 'Flash cookies' by now, given that the issue has been squarely on the FTC's radar for quite some time. Indeed, in January of 2010, FTC consumer protection Head David Vladeck announced that the FTC would soon be going after companies that use 'practices that undermine the tools that consumers use to opt out of behavioral advertising', an apparent reference to 'Flash cookies'[4]. In December 2010, the FTC issued a preliminary staff report urging web browser designers to build 'Do Not Track' options into their web browsers, in order to help consumers better protect their privacy[5]. When the report was issued, FTC Chairman Jon Leibowitz remarked that 'consumers should be able to choose whether or not to allow the collection of data about online searching and browsing'[6]. At the same time, the FTC announced that it was in discussions with Adobe, the makers of Flash software, about the problem of 'Flash cookies, and that in Chairman Leibowitz's view, 'There's an Adobe Flash problem that needs to be solved'[7].

But despite this tough talk, there has been little to no activity to date by the FTC regarding Flash cookies'. Soon after the FTC's preliminary report was issued, industry advocates and lawmakers began to express concern over the chilling effects that a 'Flash cookie' crackdown could cause. E-commerce companies warned that overly robust online privacy protections could hobble the billion-dollar online advertising industry, and could threaten the viability of a free internet[8]. One FTC commissioner suggested that the FTC's 'Do Not Track' mandate be put on ice until the FTC could more thoroughly study the potential negative ramifications of enhanced privacy protections[9], and

Despite this tough talk, there has been little to no activity to date by the FTC regarding Flash cookies'. Soon after the FTC's preliminary report was issued, industry advocates and lawmakers began to express concern over the chilling effects that a 'Flash cookie' crackdown could cause

the FTC's inaction on the issue suggests that it agrees with that notion given that it apparently has backed off of its earlier, aggressive stance.

With the lack of action by the FTC, some lawmakers are expressing impatience and frustration. On 26 September 2011, Congressmen Joe Barton (R-Texas), and Edward J. Markey (D-Mass), the Co-Chairs of the Congressional Bi-Partisan Privacy Caucus, sent a letter to Chairman Leibowitz in which they implored the FTC to take action on 'Flash cookies' by investigating and cracking down on companies that use them (the letter referred specifically to Microsoft and Hulu.com)[10]. Thus, for the time being, the ball remains in the FTC's court. When, whether and how the FTC will respond waits to be seen, leaving consumers subject to the flashing eyes of prying cookies.

Melinda F. Levitt Partner
Yonaton Aronoff Senior Counsel
Foley & Lardner
mlevitt@foley.com
yaronoff@foley.com

1. Case No. 10-Civ-9183, Memorandum and Order dated 17 August 2011.
2. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
3. No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. April 28, 2011)
4.See www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=121524
5. See www.ftc.gov/os/2010/12/101201privacyreport.pdf
6. See www.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf
7. See http://paidcontent.org/article/419-ftc-is-in-talks-with-adobe-about-the-flash-problem-/
8. See http://money.cnn.com/2010/12/02/technology/ftc_do_not_track/index.htm
9. See http://adage.com/article/guest-columnists/ftc-commissioner-thinks-track-track/149558/
10. See http://articles.law360.s3.amazonaws.com/0274000/274176/MARKEY.pdf