SPRING 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their cybersecurity, computer forensics and e-discovery needs. For this E-Newsletter, we discuss Internet cookies and the data security, privacy and legal impact it has on organizations and their employees.

Cookies and Internet Security – Emerging and Enlightening Case Law

Ancillary to the debate over which agency owns internet security and cookies regulation, are the enforcement actions undertaken in this area. In 2016, the FTC investigated 130 spyware/spam cases, and 40 general privacy cases. Their January 2017 summary of 2016 activities highlights only two cases which specifically deal with cookies. Although the FTC may be investigating the Yahoo forged cookie hack, the agency's website shows no information relating to an investigation. While the response, "We can't discuss ongoing investigations," may apply across all agencies with investigatory roles, the lack of public confirmation of such investigations is surely increasing public frustration with government efforts to promote and enforce internet security. Fortunately for users, waiting on agency enforcement proceedings for protection is not the only recourse available, and users haven't been shy about seeking redress from the courts outside of government agencies.

Murky Legal Precedent

In December 2016, a settlement was reached in IN RE: GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION (No. 1-12-md-02358), a case which revolved around Google placing cookies in web browsers which circumvented blocking settings, as well as Google's deception in statements purporting that users could prevent installation of cookies by using an "opt-out cookie," which did not prevent the installation of cookies, and in fact, sent a "hidden form" allowing the installation of certain third-party cookies. Google agreed to "expire" the cookies, effectively removing them from the affected browsers, and, create a $5.5 million settlement fund, without however, admitting wrongdoing.

Interestingly, Google had already settled a similar action with the FTC (United States v. Google Inc. (No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012)), in which Google agreed to a $22.5 million-dollar settlement in 2012, after the FTC determined Google violated a Commission Order and

placed cookies in Apple's Safari browser after an opt-out option was executed by users. The fine represented the largest FTC fine to date. In this instance, the FTC saw Google's actions as a deceptive practice, and a violation of Google's own privacy policies.

When children are added to the internet security discussion, complexity increases. IN RE: NICKELODEON CONSUMER PRIVACY LITIGATION (No. 15-1441), argued December 2015 in the Third District Court of Appeals dealt with the use of cookies to track the internet activity of children under the age of thirteen who visited the Viacom television network Nickelodeon. Despite the site's disclaimer, "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!", cookies were used to track the activity and to deliver targeted banner ads through Google's Doubleclick.net cookies.

IN RE: NICKELODEON has interesting aspect in that it demonstrates the concurrent timing on the 2015-2016 cases involving cookies and internet privacy. To quote the filed Opinion, "Google came down in November of 2015, several months after briefing in this case was complete but before oral argument... As will become clear, we conclude that Google is fatal to several of the plaintiffs' claims." What survived were privacy breach (or invasion) assertions based upon the representations that Defendants would not collect information using cookies, but did so without disclosure.

Truth in Advertising

Irrespective of the narrow scope of effective plaintiff claims, there is a track record of agency actions against entities using cookies in ways that violate consumer protection, as well as, court cases which establish the same violations. From whatever angle the subject is approached, there is an established pattern of data collection using cookies. Most of the actions and cases revolve around the cookies being used to advance targeted advertising. High end automobile companies pay to have banner ads placed on websites visited by individuals with high incomes, affluent zip codes, or luxury internet shopping transactions. Have you ever wondered how an ad for a site you visited suddenly appears on your Facebook feed? There's no magic, just cookies. Targeted advertising relies on the same logic as a luxury cruise line advertising during televised stock market reports, or a famous designer advertising in Vogue. Marketing success relies upon finding the right consumer for the product. So, why the up in arms regarding ISPs selling web browser histories, collected via cookies, on the open market?

First, the data collected isn't necessarily parsed in the same way. Vogue magazine can survey its readers anonymously, and deliver data that is ranged to potential advertisers. Advertisers will be told what the demographics look like in brackets such age, gender, income, buying preferences, etc., based upon market research. Consumers can choose not to participate in the survey, and not to buy the magazine.

In the case of ISPs collecting data from cookies, the consumer is not given the choice to "participate" simply by not answering a survey or buying a product. If you deploy a web browser or click on a site, the potential is there to collect, store, and respond to collected data on an individual basis. You will be targeted by a certain advertiser because of what websites you visited, and that advertising varies from your friends, your neighbors, your colleagues, even your spouse or child. The targeting is so specific because the information collected is so specific.

Second, cookies can be used for more than just targeted advertising. Cookies can be used to orchestrate the results of your search and direct you to specific websites, limiting your scope and access of information. An adjunct to the Net Neutrality cause, using cookies to direct web traffic

also results in directing traffic away from other sources, which is tantamount to censorship, and if allowed to happen on a for-profit basis, the deepest pockets will control the content of the internet.

Third, cookies create a trail of everything you do on the internet. If compared to the individuality of a fingerprint, the individuality of an internet search history has every probability of being equally unique (though case law relating to IP attribution is also quite murky). Many users object to the concept of “internet profiling” as an invasion of privacy. When we compound that with the idea that ISPs are permitted to sell your browser history to advertisers, is it that hard to ask why wouldn’t ISPs sell the data to potential employers? If the data is for sale legally, would it necessitate a warrant to produce it to court?

Finally, hackers already understand that the market for cookies collected data is valuable in many ways. Yahoo’s hack demonstrated the value over 32 million times with each account hacked. Hackers launch cyberattacks at ISPs daily, and we have numerous examples when ISP data security failed to stop a breach. With data for sale, it’s conceivable that a weak security link will be attached to the data eventually.

Without comprehensive regulation and enforcement of cookies, the data collected via cookies, and the resulting storage and dissemination, the protection of data, including personally identifiable data, we will be at the mercy of risk versus revenue trade-off evaluations. If there was ever a buyer beware situation, the use of cookies and the sale of internet browsing history may be one the biggest, despite a lack of current case law.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

Internet of Things World
Santa Clara, CA: May 16-18, 2017

ISSA 9th Annual Information Security Summit
Los Angeles, CA: May 18-19, 2017

ENFUSE 2017
Las Vegas, NV: May 22-25, 2017

"The Exchange" Data Privacy and Cybersecurity Forum
New York, NY: May 23-24, 2017

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: