SIDLEY AUSTIN LLP

SIDLEY

AUGUST 20, 2012

PRIVACY, DATA SECURITY AND INFORMATION LAW UPDATE

FTC Imposes Record $22.5 Million Fine on Google for Violation of Prior Privacy Promises

The Federal Trade Commission ("FTC") announced on August 9, 2012 that Google Inc. ("Google") agreed to pay a $22.5 million civil penalty to settle allegations that the company had breached default settings on Apple Inc.'s Safari browser by placing tracking cookies and serving targeted advertisements to users in conflict with Google's specific, public representations to the contrary.[1] The FTC claimed that this alleged wrongdoing, which Google explicitly denied in the proposed order, violated the terms of the 2011 Google "Buzz" consent decree.[2] Google entered into the consent decree to pay the civil penalty and take remedial measures to remove its cookies from user devices, but denied liability for all of the Commission's allegations regarding its activities. Significantly, the FTC did not even allege that anyone was harmed by Google's practices, or that the relevant cookie-placement, tracking or information collection would have been illegal but for Google's violation of its prior consent decree and its affirmative misrepresentations.

In the complaint filed in the Northern District of California,[3] the FTC charged Google, the operator of the world's largest Internet search engine, with placing advertising tracking cookies on the computers of Safari users who visited sites affiliated with Google's DoubleClick advertising network, despite prior statements by Google to these users that the users would be opted-out of tracking as a result of the Safari browser's default settings. Specifically, the FTC alleged that Google explained to Safari users that the Safari browser would block third-party cookies by default and that this setting "effectively accomplishes the same thing" as opting out of a Google advertising tracking cookie. The FTC also cited the fact that Google was at the time a member of the Network Advertising Initiative ("NAI"), an industry self-regulatory organization that requires members to adhere to a code of conduct that includes the disclosure of their data collection and use practices. It is significant that the FTC included the NAI count in its complaint against Google because this reflects the agency's willingness to enforce industry self-regulatory standards. This point is an important element—and expectation—of the White House's Privacy Blueprint, released in February 2012.

The FTC alleged that, in spite of these representations and its membership in the NAI, Google placed its advertising tracking cookies on consumers' computers, often by circumventing the default Safari browser settings by exploiting an exception in the Safari browser settings that allowed a temporary cookie from Google's DoubleClick advertising domain to effectively open the door to other DoubleClick cookies. Importantly, James Kohm, Associate Director of

---

[1] *See* FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), http://ftc.gov/opa/2012/08/google.shtm.

[2] *See In the Matter of Google Inc.*, FTC File No. 102-3136, Docket No. C-4336 (Oct. 13, 2011).

[3] *See* Complaint, *United States v. Google*, N.D. Cal., filed Aug. 8, 2012.

the FTC Bureau of Consumer Protection's Division of Enforcement, expressly noted in the FTC's press conference that the violations in the Complaint were based only on affirmative "misrepresentation" of privacy practices by Google, and not on the collection of user data through cookies.

The $22.5 million fine is the largest penalty the FTC has ever obtained for a violation of a Commission order, eclipsing the $15 million fine imposed on data broker ChoicePoint Inc. in 2006.[4] Under the proposed consent decree, Google will, in addition to paying the civil penalty of $22.5 million, be required to maintain through February 15, 2014 "systems configured to instruct Safari-brand web browsers to expire any DoubleClick.net cookie," other than opt-out cookies, placed by Google dating through February 15, 2012. James Kohm suggested that the 2014 date would provide enough time for Google to remove cookies when users visit Google or Google-affiliated sites. (Cookies can generally be "expired" or removed when a user's browser visits the site that originally placed the cookie.)

The heavy fine imposed upon Google should be viewed in the context of Google's size and the 2011 consent decree the company entered into with the FTC regarding privacy violations in the deployment of the short-lived Google Buzz social networking tool. In the 2011 consent decree, Google settled charges that it violated Section 5 of the FTC Act by engaging in deceptive tactics and misrepresenting the privacy practices of the Buzz tool to users. Under the terms of the 2011 decree, Google was barred from future privacy misrepresentations, required to implement a comprehensive privacy program, and subjected to regular, independent privacy audits over a twenty year period. The 2011 consent decree's ban on future privacy misrepresentations appears to have served as the trigger for the FTC's action in the Safari cookie consent decree, and is featured prominently in the Commission's Complaint.

In large part, the record-setting fine appears to be aimed at sending "a clear message to all companies under an FTC privacy order," as FTC Chairman Jon Leibowitz explained. Indeed, in a Commission Facebook "chat" following the announcement of the settlement, FTC Division of Enforcement staff explained that the settlement is significant because "Google is paying with black eyes as well as greenbacks. We will continue watching them and there will be increasing deterrence as needed." It appears that the FTC intends for this settlement to serve as a warning to the large number of internet, online media and other technology firms operating under FTC consent orders of the potential repercussions of additional violations.

Commissioner J. Thomas Rosch dissented from the Commission's acceptance of the consent decree, arguing in his Dissenting Statement that the consent decree was not in the "public interest" because it contained, without providing an adequate explanation of Commission's acceptance of, a full denial of liability by Google. In Commissioner Rosch's view, the Commission should not have condoned or accepted Google's denial of liability, particularly given that this violation, following on the heels of the 2011 Google Buzz consent order, was "Google's second bite at the apple" and tantamount to a contempt charge. Given his view that there was "no question…that there is 'reason to believe' that Google is in contempt of a prior Commission order," Commissioner Rosch suggested that Google's denial of liability set a poor example for future respondents who may also seek to deny liability in consent decrees.

Alan Raul
araul@sidley.com
+1.202.736.8477

Edward McNicholas
emcnicholas@sidley.com
+1.202.736.8010

The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes lawyers experienced in regulatory compliance, litigation, financial institutions, healthcare, EU regulation, IT licensing, marketing counsel, intellectual property, and criminal issues. Sidley provides services in the following areas:

[4] The ChoicePoint settlement included $10 million in civil penalties and $5 million in consumer redress payments. *See United States of America v. Choice Point Inc.*, Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, FTC File No. 052-3069 (N.D. Ga. Jan. 26, 2006).

- Privacy and Consumer Protection Litigation, Enforcement and Regulatory Compliance
- Data Breach, Incident Response, and Cybersecurity Advice
- Global Data Protection, International Data Transfer Solutions and Cross-Boarder Issues
- Corporate Data Protection, Compliance Programs and Information Governance Assessments
- FTC and State Attorney General Investigations of Unfair or Deceptive Acts and Practices
- Social Media, Cloud Computing, Online Advertising, E-Commerce and Internet Issues
- EU, China and Japan Data Protection and Compliance Counseling
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Communications Law and Data Protection
- Workplace Privacy and Employee Monitoring
- Website Policies Online Trademarks and Domain Name Protection
- Records Retention, Electronic Discovery, Government Access and National Security

To receive future copies of this and other Sidley updates via email, please sign up at www.sidley.com/subscribe