THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP/US
October 2012 • Volume 12 • Number 8

FTC ramping up data privacy enforcement actions; Google fined $22.5 million

By David M. Governo and Corey M. Dennis, CIPP/US

Last month, Google agreed to pay a $22.5 million civil penalty to settle Federal Trade Commission (FTC) charges claiming it misrepresented to users of Apple's Safari Internet browser that it would not place advertising tracking "cookies" or serve targeted ads to them in violation of an earlier privacy settlement it reached with the FTC. According to a recent FTC press release, this represents the largest FTC penalty ever for a violation of a commission order.

The FTC's complaint alleged that Google placed advertising tracking cookies onto users' Safari browsers for several months in 2011 and 2012, which enabled Google to collect user information and serve targeted advertisements to them, even though it had previously told them that they would be opted out of such tracking. The FTC also charged that Google's misrepresentations violated the October 2011 Google Buzz settlement, based on alleged deceptive privacy practices relating to the now-defunct Google Buzz social network, which barred it from future privacy misrepresentations, required it to implement a comprehensive privacy program and required independent privacy audits for 20 years. Google has denied liability, calling the use of tracking cookies an inadvertent technical glitch, but has agreed to pay the $22.5 million penalty.

The commission voted to approve the proposed consent decree, stating that the settlement is "intended to provide a strong message to Google and other companies under order that their actions will be under close scrutiny and that the commission will respond to violations quickly and vigorously." Commissioner J. Thomas Rosch dissented, arguing that a consent decree containing a denial of liability should not be accepted and that "$22.5 million represents a *de minimis* amount" of Google's $38 billion annual revenues, nearly all of which are derived from advertising. However, the majority of the commission disagreed, explaining that a denial of liability is not "inconsistent with the imposition of a civil penalty" and the "swift imposition of a $22.5 million fine helps promote" future compliance.

The FTC's complaint alleged violations of Section 5 of the FTC Act, 15 U.S.C. § 45, which bars "unfair or deceptive acts or practices in or affecting commerce." A host of other laws provide the agency with enforcement authority to protect consumers' privacy, including the Gramm–Leach–Bliley Act, applicable

to financial institutions; the federal Red Flags Rule, applicable to financial institutions and certain other creditors, and the Children's Online Privacy Protection Act, applicable to commercial websites and online services directed to children.

In recent months, the FTC has ramped up its enforcement of data privacy laws, which is clear from the following:

- The FTC approved a final settlement with Facebook resolving charges that Facebook deceived consumers by sharing their information with others—including advertisers—and making it public after informing them that it would remain private. The settlement requires Facebook to give consumers clear notice and obtain their express consent before sharing their information, maintain a comprehensive privacy program to protect their information and obtain biennial privacy audits from an independent third party.

- The FTC filed a complaint against Wyndham Hotels in June charging that it misrepresented its information security measures and repeatedly failed to safeguard consumers' personal information, which resulted in the compromise of several hundred thousand consumers' payment card data and a $10.6 million loss due to fraud.

- In March, RockYou, the operator of a social game site, agreed to settle charges that it failed to protect the privacy of its users, despite its representations to the contrary, allowing hackers to access the personal information of 32 million users—including 179,000 children—in violation of Section 5 of the FTC Act and the Children's Online Privacy Protection Act Rule. The settlement requires the company to pay a $250,000 civil penalty, maintain a data security program and submit to security audits for 20 years.

- In June, the FTC reached settlements with a debt collection business and an auto dealer charged in separate cases with failing to maintain reasonable security measures to protect consumers' personal information and exposing that information by installing peer-to-peer file-sharing software on their corporate computer systems. The settlements with both businesses bar them from making misrepresentations about the privacy and security of consumers' personal information and require them to maintain comprehensive information security programs.

The FTC has issued numerous press releases reporting these and other privacy enforcement actions and settlements. These developments, which have also been reported in major news outlets—including *The Wall Street Journal, The New York Times*, and *The Washington Post*—underscore the importance of maintaining appropriate safeguards to protect personal information.

In March, the FTC issued a report entitled *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* setting forth best practices for companies to protect consumer privacy, including Privacy by Design, building in privacy protections at every stage of product/service development; simplified consumer choice regarding information sharing, including do-not-track mechanisms, and greater transparency, disclosing details about collection and use of consumers' information.

Given the trend of active data privacy law enforcement at both the state and federal level, companies would be wise to follow these guidelines.

David M. Governo is the founding partner of Governo Law Firm LLC, an 18-attorney law firm in Boston, MA. For over three decades, he has advised companies on a range of risk management and compliance issues and defended companies in complex litigation. He has attained Martindale-Hubbell's highest "AV" rating, is an

active member of the Federation of Defense and Corporate Counsel and has been voted a New England Super Lawyer for many years.

Corey M. Dennis, CIPP/US, defends companies in complex litigation and advises companies on risk management and compliance issues at Governo Law Firm LLC. He has counseled businesses on compliance with data privacy laws, is a Certified Information Privacy Professional (CIPP/US) and has published numerous legal articles in the areas of data privacy, civil litigation, social media, toxic tort and employment law.