Advisory

FEBRUARY 2013

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

JONATHAN MEDALSY
212.551.2637
jmedalsy@wiggin.com

PRIVACY AND INFORMATION SECURITY PRACTICE GROUP

Wiggin and Dana's Privacy and Information Security Practice is a multi-disciplinary team of seasoned attorneys from a wide-range of practices, including Technology and Outsourcing, Litigation, Health Care, Franchise, Antitrust and Consumer Protection, Insurance, and White Collar Defense, Investigations and Corporate Compliance. Because of this breadth and diversity of experience, our Privacy and Information Security Practice is able to provide effective, strategic and industry-tailored advice to a broad array of national and international clients.

The Federal Trade Commission's 'Device Squad' Gets Technical with HTC on Smartphone Security

For several years running, the Federal Trade Commission ("FTC" or "Commission") has chastened businesses for alleged laxity in securing consumer data from breaches and other unauthorized access. The overwhelming majority of these enforcement efforts have focused on how corporate end users of information technology products fail to manage the security of their internal networks or fail to undertake basic administrative precautions, such as periodic data risk assessments and employee security training programs. More recently, the FTC has turned its attention to privacy and security lapses in mobile apps that run on smartphones and tablets.[i] Last Friday, however, with its announced settlement[ii] with smartphone manufacturer HTC America, Inc. ("HTC"), the FTC has donned a white frock coat, grabbed its quality assurance clipboard and marched into the design labs of mobile handset makers to deliver a warning about data vulnerabilities in the manufacture of mobile devices. With this unprecedented enforcement action against a mobile device maker, the FTC has signaled that its self-named "Device Squad" is not afraid to get geeky in pursuing unfair data practices in the mobile industry.

ALLEGED SECURITY WEAKNESSES IN HTC'S CUSTOMIZATION OF MOBILE DEVICES

HTC makes smartphones and tablets that run on Google and Microsoft-developed operating systems (e.g., Google's Android and Microsoft's Windows Mobile systems). HTC customizes the devices it manufactures to help differentiate them from competing devices and to meet certain requirements of wireless carriers such as Sprint Nextel and AT&T. These customizations include pre-installed applications that customers do not choose to install and that cannot be uninstalled by users once they have purchased the device.

The FTC alleges that software customizations in devices made by HTC effectively undermined privacy and security controls that had been built into the Google and Microsoft operating systems that run on the devices. A key feature of these operating system controls requires that a device user be notified and allowed to consent before an app collects or shares sensitive information from her device (such as the content of text messages, user contacts lists, G-mail accounts and web-viewing history). Similarly, such controls require notice and consent before sensitive device functions (such as voice-recording or geo-location capabilities) can be activated by other apps that are installed on a mobile device. Such controls are otherwise known as "permission-based security." The FTC charges that HTC circumvented these and other operating system controls by:

- Failing to include "permission-check" codes in its custom applications. This failure then allowed other apps installed on HTC devices to access sensitive user

CONTINUED ON NEXT PAGE

The Federal Trade Commission's 'Device Squad' Gets Technical with HTC on Smartphone Security CONTINUED

data and functions without the user's knowledge or consent. One example of this "permission re-delegation" vulnerability cited by the FTC involved an HTC-installed voice-recording app that allowed other apps to access the device's microphone, even if the user's permission was not requested. A piece of malware could exploit this "hole" in an HTC device to secretly record conversations. In effect, these HTC applications risked handing over the keys to a user's sensitive information and device functions to any other app that "asked" for them;

- Pre-installing custom software on Android devices which the downloading of other apps onto a device (i) outside the usual Android installation process and (ii) without user knowledge or consent, again circumventing the permission-based security process that would normally apply in the Android operating system;

- Deploying software applications that create detailed logs of a device for trouble-shooting and diagnostic purposes, but failing to use well-known mechanisms to ensure that sensitive log information could be accessed only by HTC- designated applications or authorized carriers. The result was vulnerability to unauthorized access to sensitive information by third party apps and exposure to well-known mobile malware attacks, such as sending text messages without permission (e.g., 'toll fraud');

- Shipping the HTC devices without first de-activating certain debugging code used during the manufacturing process. The result was that sensitive information continued to be written to device system logs (unnecessarily) and accessible to any third party apps on the devices that could access the internet;

- Not following security practices described in the operating system guides provided by Google and Microsoft for device manufacturers;

- Not testing the customized software on HTC devices for potential security vulnerabilities before shipping the devices and not responding to warnings about security flaws.

Collectively, in the FTC's view, these HTC practices constituted an unfair trade practice through failure to provide "reasonable and adequate security in the design and customization" of the software HTC installed on its mobile devices. Or, as the FTC put it more succinctly in a press release, "The company didn't design its products with security in mind." The FTC also complained that certain representations by HTC in its user manuals regarding security controls were false or misleading.

The terms of the proposed consent order[iii] include a requirement that HTC implement a comprehensive information security program, including measures to assess risks to security and confidentiality of "covered information"[iv] in the development of its products and related custom software. Other remedies include the development of security patches for the alleged security vulnerabilities in HTC's custom software as well as ongoing third party audit and reporting requirements.

CONTINUED ON NEXT PAGE

The Federal Trade Commission's 'Device Squad' Gets Technical with HTC on Smartphone Security CONTINUED

THE FTC'S ENFORCEMENT RATIONALE AND IMPLICATIONS FOR THE MOBILE INDUSTRY

The HTC enforcement action represents the first time the FTC has taken on a device manufacturer in the deeply technical realm of software configurations for mobile privacy controls. In part, the action may reflect the FTC's growing confidence in its understanding of the mobile services industry and in the ability of FTC staff to cite companies that deviate significantly from 'industry standards' to the detriment of consumers. That confidence has been challenged in one recent FTC action, where the respondent hotel chain has moved to dismiss on the grounds that FTC actions of this kind outstrip the Commission's authority under Section 5 of the FTC Act and violate the Commission's own rulemaking procedures.[v] It remains to be seen whether this challenge will throw a wrench into the FTC's now well-established campaign against subpar private sector data security practices.

Regardless of how well the FTC is feeling its oats in this area, the HTC case signals a recognition that 'privacy by design' in the mobile sector is inherently complex and depends upon commonly accepted technical protocols that are respected by device makers as well as by operating system developers, carriers and app developers. We have probably not heard the last from the FTC's Device Squad.

[i] http://www.wiggin.com/federal-trade-commission-issues-comprehensive-mobile-privacy-recommendations-

[ii] http://www.ftc.gov/opa/2013/02/htc.shtm

[iii] The consent order is subject to 30 days for the taking of public comments. As with all such consent orders, the respondent HTC neither admits nor denies the allegations in the FTC's underlying complaint.

[iv] "Covered information" includes a broad list of individually-identifiable information collected by or stored on HTC devices. See the proposed consent order, Definitions, paragraph 2: http://www.ftc.gov/os/caselist/1223049/130222htcorder.pdf

[v] See Wyndham Hotels Worldwide Corporation motion to dismiss the FTC's complaint at http://www.chamberlitigation.com/sites/default/files/cases/files/2012/Wyndham%20Motion%20to%20Dismiss%20(MTD)%20--%20FTC%20v.%20Wyndham%20Worldwide%20Corp.,%20et%20al.%20(U.S.%20Dist.%20Court%20for%20Dist.%20of%20Arizona).pdf