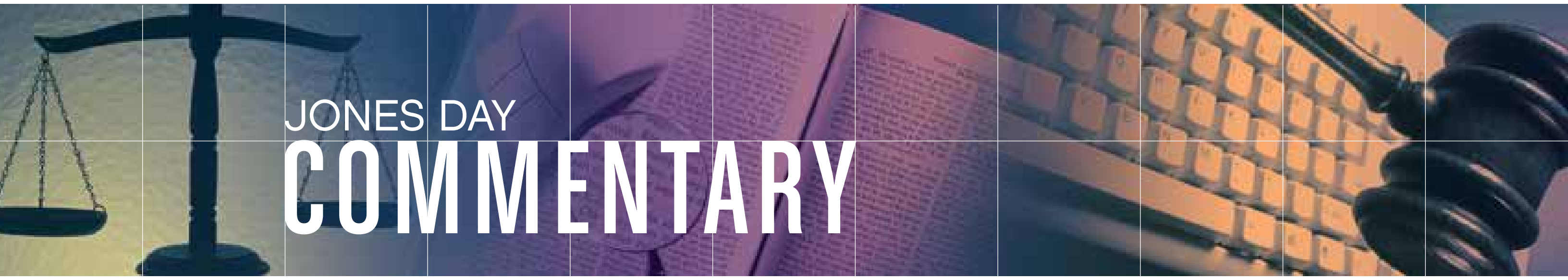
MARCH 2013



JONES DAY
COMMENTARY

LESSONS FROM *IN RE HTC AMERICA INC.*: FTC'S BROADENING APPROACH TO CONSUMER DATA SECURITY LEAVES UNWARY MANUFACTURER OR DEVELOPER WITH MORE THAN IT BARGAINED FOR

The Federal Trade Commission's ("FTC") recent enforcement action *In the Matter of HTC America Inc.* ("HTC"), **FTC File No. 1223049**, illustrates the FTC's broadening approach to regulating reasonable data security practices and consumer protection. The FTC's traditional enforcement action in the area of consumer privacy and data security protection has focused on companies with direct contact with consumers. The complaint and **consent order** in *In the Matter of HTC America Inc.* is significant because it involves component manufacturers and software developers who provide the solutions used to store, process, or otherwise interact with consumer personal data. As a result of this consent order, a much broader range of companies needs to consider the privacy and data security implications of developing custom applications and software interfaces for consumer products.

THE COMPLAINT

HTC is a mobile device manufacturer whose portfolio includes smart phones and tablets powered by the Android and Windows Phone mobile operating systems. The FTC charged HTC with failing to employ "reasonable security measures" in the customization of software used in certain mobile devices running these operating systems. Although these devices were sold to consumers by network operators, the FTC charged HTC with unfair and deceptive business practices related to security and privacy violations in connection with HTC's creation and modification of preinstalled applications, and HTC's representations made in the devices' user manuals and interfaces.

Allegations. In support of its position that HTC engaged in unfair and deceptive business practices in violation of consumer protections, the FTC complaint alleged that HTC: (i) failed to implement an adequate program to assess the appropriateness of the security features in its mobile devices; (ii) failed to implement adequate data privacy and security guidance or training for its engineering staff; (iii) failed to conduct ongoing assessments and reviews to identify potential security vulnerabilities in its mobile devices; (iv) failed to follow well-known and commonly accepted secure coding practices; and (v) failed to implement a process for receiving and addressing security vulnerability reports from researchers, academics, or the public.

Permissions and Re-Delegation. The primary focus of the FTC's complaint was HTC's various actions and inactions that allegedly undermined Android's permission-based security model. The Android operating system employs a permission-based approach to restrict access by third-party applications to certain information (e.g., location information or the contents of text messages) and device functionality (e.g., the ability to record audio through the device's microphone or take pictures with the device's camera). Third-party applications are required to declare, during the installation process, what information or functionality they access, and request a user's permission prior to such access.

The FTC contended that HTC undermined Android's permission-based security model by introducing "permission re-delegation" vulnerabilities through its own custom applications that it preinstalled on each device. This custom software allowed third-party applications to access sensitive information and functionalities without receiving permission from the user. For example, the FTC alleged that HTC preinstalled a custom voice recorder on its devices that, if exploited, enabled third-party applications to access the device's microphone, without requesting permission from the user.

Similarly, the FTC alleged that HTC preinstalled a download application that enabled third-party applications to install any additional applications from any server onto the device without the user's knowledge or consent by bypassing the Android permission-based security installation protocol. Because the preinstalled download application installs applications outside the normal Android application installation process, the FTC alleged the user would not be notified of what sensitive information or functionality the application would access. The FTC alleged that this vulnerability "undermine[d] all protections provided by Android's permission-based security model."

Despite these alleged security deficiencies, HTC's user manuals for its Android-based mobile devices discussed Android's permission-based security model and informed consumers that applications installed from the Android marketplace require permission to access personal information or sensitive device functions.

Insecure Communications Mechanisms. Another significant security threat alleged by the FTC was the insecure communications mechanisms HTC utilized in implementing the HTC Logger and Carrier IQ logging applications on its devices. These logging applications saved important information regarding a user and the device, including GPS and network locations, web-browsing and media-viewing history, the user's personal phone number, text message content, and any other usage and device information specified for collection by network operators. The FTC contended that the communications mechanisms used to process and analyze the logging data were unencrypted, and thus any third-party application with internet access could access the sensitive information contained on the loggers, rendering the device and such data insecure.

Debug Code. The FTC also alleged that HTC failed to deactivate the debug code it used to develop and test its implementation software for the Carrier IQ logging application. As a result, all information sent to Carrier IQ by such software was written to the Android system log. This information was then viewable by any third-party application with permission to read the log, and included GPS-based location, web-browsing and media-viewing history, and the content of incoming text messages. This information was also provided to HTC whenever a user chose to send error reports using the "Tell HTC" error reporting tool, even where the user to declined consent to the transmission of location information to HTC.

Claims. The FTC claimed HTC's practices constitute unfair business practices by causing, or being likely to cause, substantial injury to consumers, including potential financial harm (due to compromised bank information, personal history information, text message fraud) and physical harm (by possibly physically tracking or stalking individuals by manipulating sensitive device functionalities).

It also alleged that HTC engaged in deceptive business practices by making false or misleading representations concerning data and device security in its user manuals, while including custom applications that circumvented the operating system's permission-based security model.

Finally, the FTC charged HTC with using a deceptive user interface with regard to its "Tell HTC" reporting tool, which purported to require user consent to transmit location data to HTC, but which transmitted the data without such consent.

THE CONSENT ORDER

Without admitting fault, HTC stipulated to a 20-year term consent order to settle the enforcement action. Like many FTC consent orders, this consent order requires HTC to establish a comprehensive security program designed to address security risks relating to devices and consumer data. The consent order and settlement require HTC to identify and implement a wide-ranging protocol throughout its mobile devices business, including:

- Designating employees to coordinate and be accountable for the security program;
- Identifying internal and external risks to the security of mobile devices that could result in unauthorized access to, or use of, device functionality (and continuously assessing the risks);
- Identifying material internal and external risks to the security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information (and continuously assessing the risks);
- Designing and implementing reasonable safeguards to control the risks identified through the risk assessments, including through reasonable and appropriate software security testing techniques, and regular testing or monitoring of the security program; and
- Developing and using reasonable steps to select and retain service providers capable of maintaining security practices consistent with the consent order.

The consent order also requires HTC to issue security patches to address the security vulnerabilities identified in the complaint. Additionally, HTC is required to develop record retention, notice, and reporting processes to ensure its compliance with the consent order and hire a qualified, objective, independent third-party professional to assess, evaluate, and issue reports regarding its security program every two years during the consent order's 20-year term. The consent order is currently open for **public comment**, with comments due by March 22, 2013.

IMPLICATIONS

Many original equipment manufacturers and device application providers collect device and certain user data to improve their products and, in some cases, establish a direct relationship with consumers through product registrations, warranty support, and device use analytics. As illustrated by the FTC's complaint, the entire chain of companies connected with consumer products, especially those that implicate the collection and storage of consumer data, are expected to employ reasonable device and information security practices. Manufacturers and developers are expected to implement a reasonable design and development process that adopts reasonable security practices to avoid introducing security risk into consumer products. This recent FTC enforcement action shows that even manufacturers and developers with limited contact with consumers face data privacy and security consumer protection enforcement risks.

Also, the FTC's policy of "security by design" now clearly applies to any number of "upstream" activities that can affect the consumer. Companies must therefore address privacy and data security issues when developing custom applications and software interfaces for consumer products. Such applications and interfaces should also include privacy policies where the associated device collects and stores data about the customer, because enforcement agencies often link together issues relating to privacy and security.

In the case of HTC, software development was alleged to have provided access to sensitive information both directly (microphones, etc.) and through logging applications and error reports. To the FTC, inadequate post-development controls (such as the failure to have a security checklist or other control mechanism to detect that the debugging code had not been deactivated), and the lack of appropriate monitoring and audit procedures, compounded the development problems and delayed detection and correction of the security flaws. Accordingly, in addition to considering security at the development stage, it is equally important for companies in the supply chain to establish security procedures connected to ongoing post-development product monitoring.

This consent order also has implications for any original manufacturers and developers and upstream companies that provide communications to consumers relating to data, device, and application security. All notices, user manuals, information sheets, and other information shared with consumers directly by such companies must accurately reflect the product's security to avoid potential false or misleading representation allegations. This will become increasingly important for companies that traditionally have not established a direct consumer relationship through data collection and installed applications, but that increasingly see significant value in such relationships.

In sum, original manufacturers and upstream developers must take stock of the data security issues implicated by their products and programs. Security should be considered at each stage of development, with attention to reasonable, industry-standard security principles and practices. These include utilizing appropriate notice and consent procedures, limiting collection and storage of information, protecting collected information through encryption or other reasonable procedures, and having reasonable procedures to identify and remedy security threats. The FTC business guide, ***Mobile App Developers: Start with Security***, provides additional information software developers may find useful in implementing reasonable security measures.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Katherine S. Ritchey
San Francisco
+1.415.875.5728
ksritchey@jonesday.com

Gregory P. Silberman
Silicon Valley
+1.650.739.3954
gpsilberman@jonesday.com

Mauricio Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

The authors would like to thank Amir Amiri, an associate in the San Francisco Office, for his assistance in the preparation of this Commentary.

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our web site at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.