Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Practical Privacy Takeaways From FTC's Deal With HTC

Law360, New York (March 04, 2013, 12:59 PM ET) -- Consistent with the Federal Trade Commission's laser focus on mobile privacy, the commission recently announced its latest privacy law enforcement action — this time against a mobile device manufacturer. The announcement, with HTC America Inc., involves the FTC's charges that the device manufacturer did not sufficiently secure the software that it developed for its smartphones and tablet computers, and did not accurately describe its data handling practices to device users.

The FTC's allegations underscore the commission's view that companies are required under Section 5 of the FTC Act to (1) implement a number of specific privacy-by-design steps to products capable of collecting, accessing, and transmitting personal information, and (2) carefully confirm that any representations they make about a product and how personal information is handled — including statements in a product's user guide and representations made on the interface of a software application — remain consistent with the product's capabilities.

The case is a good example of how quickly and aggressively privacy law and enforcement are evolving, and how important it is to be cognizant of such legal trends and how they affect a company's privacy responsibilities in product design and development. The failure to incorporate such considerations from "the ground up" and as part of a company's culture, training and oversight — as evidenced by the FTC's steady enforcement on such issues — can, as evidenced by this action and others, lead to 20-year regulatory consent orders and/or expensive litigation.

This article outlines the FTC's most recent "privacy by design" law enforcement action, and identifies several practical tips to keep in mind for companies that design and market products capable of collecting, storing or disclosing personal information.

The FTC's Complaint — Product Design Closely Scrutinized

By way of background, the device manufacturer at issue in today's FTC action customizes Android and Windows-based mobile devices. Such customization allows the manufacturer to differentiate its products from competitors, and also to ensure that the products satisfy additional requirements that might apply through arrangements with various wireless carriers that sell such devices to consumers. In this matter, the FTC claimed that the manufacturer modified original settings of the Android and Windows-based devices in such a way that introduced unreasonable security vulnerabilities.

The FTC's complaint focused on three particular product modifications that, in its view, were "unfair" under Section 5 of the FTC Act. This is the first case in which the FTC has alleged such specific actions or omissions in product design are unlawful.

Permission Redelegation Charges

The FTC first took issue with what it termed as the company's "permission redelegation" modification in the devices. The FTC explained that "permission re-delegation" occurs when one application that has permission to access certain types of personal information[1] (or where the mobile device can capture, access or transmit such personal information) delegates that permission authority to another application that does not have the same level of access or functionality permission.

In other words, a user grants consent for Application A to access the device's precise geolocation information, but did not provide consent to Application B to access such information. Through a modification setting in the device, Application B can use the permission granted to Application A to access precise geolocation information on the device.

Here, the FTC claimed that, because the company, in several ways, did not include a "permission check" code in its custom, pre-installed applications on its Android-based devices (i.e., a confirmation that an application has permission to access certain sensitive information or functionality on the device), the absence of such a safeguard allowed any third-party application to command the device's custom applications to access various personal information and device functionality on the third party's behalf — including enabling the device's microphone, accessing the user's GPS-based, cell-based, and Wi-Fi-based location information, and sending text messages, and that such commands could occur by the third party without requesting the device user's permission.

Application Installation Vulnerability Charges

The FTC next took issue with the company's pre-installation of a custom application on its Android-based devices that could download and install applications outside of the normal Android installation process, in which the default setting is for permission to be sought and granted by the user before applications will be installed on the device. That is, under the permission-based security model, before a user installs a third-party application, the Android operating system provides notice to the user regarding what sensitive information or device functionality the application states it requires, and the user must opt in to such data collection or access to complete installation of the third-party application.

Here, the FTC claimed that the company did not include appropriate permission check software code to protect the custom pre-installed application from third-party exploitation. As a result, the FTC claimed that any third-party application could command the pre-installed application to download and install additional applications from any server onto the device without a user's knowledge or consent.

Insecure Communications Mechanism Charges

The third design issue, in the FTC's view, was the company's failure to use "readily-available and documented secure communications mechanisms in implementing logging applications on its devices," which the FTC claimed put personal information at risk. These logging mechanisms involved customer support, trouble-shooting, as well as diagnostics. In the FTC's view, a device's "communications with logging applications should be secure to ensure that only designated applications can access the information."

Based on the above, the FTC alleged that, for about one year (between late December 2010 until late 2011), the company failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices because, among other things, it:

- did not implement an adequate program to assess the security of products it shipped to consumers;

- did not implement adequate privacy and security guidance or training for its engineering staff;

- did not conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices;

- did not follow well-known and commonly accepted secure programming practices, including secure practices that were expressly described in the operating system's guides for manufacturers and developers, which would have ensured that applications only had access to users' information with their consent; and

- did not implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.

As a result of not taking such steps, the FTC charged that millions of the company's mobile devices compromised sensitive device functionality, potentially permitting malicious applications to send text messages, record audio, and install additional malware onto a consumer's device without the user's knowledge or consent. The FTC alleged that malware placed on consumers' devices without their permission "could be" used to record and transmit information entered into or stored on the device, including, financial account numbers and related access codes or medical information such as text messages received from healthcare providers and calendar entries concerning doctor's appointments. In addition, the FTC noted it was possible that malicious applications could exploit the vulnerabilities on the devices to gain unauthorized access to a variety of other sensitive information, such as the user's geolocation information and the contents of the user's text messages.

Count One of the Complaint (Unfairness)

These omissions and the resulting potential consumer injury formed the basis for the complaint's "unfairness" claim under Section 5 of the FTC Act (Count I). Specifically, the FTC alleged that, as a result of such actions/inactions, the company "failed to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices," and that the company's "practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice."

Counts Two and Three of the Complaint (Deception)

The FTC's complaint also alleged two "deception" claims under Section 5 of the FTC Act (Counts II and III). In a novel approach, the complaint's deception allegations were based, not on statements made in a privacy policy, but on statements contained in the company's user manuals for its Android-based devices and in an application's user interface.

- User Guide Claims: The FTC claimed that the company represented expressly or implicitly in its product user guides that, through the Android permission-based security model, device users would be notified when a third-party application required access to personal information or device functions. Yet, the FTC alleged that users were not always so notified and had not provided consent to such third-party access. For this reason, the FTC charged that such statements in the device's user guide were deceptive.

- User Interface Claims: The FTC also claimed that, in the device's troubleshooting application user interface, the company represented that if a user did not affirmatively opt in to "add location data" when submitting an error report through the application, then location data would not be sent to the company with the user's error report. In some instances, even if a user did not opt in to share such information, the FTC asserted that geolocation data was still sent to the company with the error report. For this reason, the FTC charged the user interface representation about sharing geolocation information was deceptive.

Settlement Provisions

Most of the provisions outlined below apply to the company for 20 years, and a violation of such provision could subject the company to civil penalties of up to $16,000 per violation.

Advertising Injunction

The settlement prohibits the company or its agents from misrepresenting the extent to which the company, or any of its products or services, maintain and protect the security of a mobile device's ability to capture, access, or transmit personal information (as defined by the order, noted above), or the security, privacy, confidentiality, or integrity of any personal information from or about consumers.

Comprehensive Security Program

The settlement requires the company to establish, implement, and maintain a comprehensive written security program designed to (1) address security risks related to the development and management of new and existing mobile devices, and (2) protect the security, confidentiality and integrity of personal information collected by the company and input into, stored on, captured with, accessed and/or transmitted through the company's mobile devices. The program must contain administrative, technical and physical safeguards appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the device functionality or personal information, including the specific requirements identified below.

- Security Program Lead: The company must designate an employee or employees to coordinate and be accountable for the security program.

- Product and Data Risk Assessments: The company must perform a risk assessment that identifies material internal and external risks to the security of its mobile devices that could result in unauthorized access to or use of device functionality, and assessment of the sufficiency of any safeguards in place to control these risks. The company also must perform risk assessments to identify material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of such information, whether such information is in the company's possession or is input into, stored on, captured with, accessed or transmitted through one of its devices, and assess the sufficiency of any safeguards in place to control these risks. These risk assessments, at a minimum, must consider risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development and research; (3) secure software design and testing, including secure engineering and defensive programming; and (4) review, assessment, and response to third-party security vulnerability reports;

- Safeguard Design Resulting from Risk Assessments: The company must design and implement reasonable safeguards to control the risks identified through its risk assessments, including through reasonable and appropriate software security testing techniques, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems and procedures;

- Vendor Program: The company must develop and use reasonable steps to select and retain service providers capable of maintaining security practices consistent with the consent order requirements, and require service providers by contract to implement and maintain appropriate safeguards; and

- Dynamic Security Program: The company must evaluate and adjust the security program in light of the results of the testing and monitoring required by the above terms, any material changes to the company's operations or business arrangements, or any other circumstances that the company knows or has reason to know may have a material impact on the effectiveness of its security program.

The settlement excludes from its coverage any responsibility to identify and correct security vulnerabilities in third-party software on the company's devices to the extent the vulnerabilities are not the result of respondent's integration, modification, or customization of the third party software.

Security Patch Requirement — Remediation

The settlement also requires that the company develop security patches to fix the three types of security vulnerabilities identified (e.g., permission redelegation, application installation vulnerability and insecure communication mechanisms) for each affected covered device having an operating system version released on or after December 2010, and that such security patches shall be released within 30 days of service of this order either directly to affected devices or to the applicable network operator for deployment of the security patch(es) to the affected devices. The company also must provide users of the affected devices with clear and prominent notice regarding the availability of the applicable security patch(es) and instructions for installing the applicable security patch(es).

20-Year Independent Security Audit and Reporting Requirements

The settlement further requires that the company hire a qualified third-party professional to audit the company's security program to confirm compliance with the requirements of the settlement order, and to provide reports to the FTC of the audit every other year for 20 years. The settlement also requires various reporting and notice requirements, consistent with past FTC orders.

Practical Privacy Tips

Privacy Review in Product Design — Some Things To Look For

There are numerous examples where a company's selected default (or modified) settings in collecting personal information backfired for the company beyond this most recent case, including GoogleBuzz (beta program that defaulted to gmail users being opted into social network, FTC investigation and settlement);Sears Roebuck (collected sensitive personal information through software without sufficient disclosure, resulting in an FTC investigation and settlement);Facebook Inc. (changed users' settings over certain information from private to public, resulting in FTC investigation and settlement); and FitBit (sensitive health data logged via fitness device appeared on Internet searches where the online journals were set to public settings by default, causing a PR problem for the startup).

One of the lessons from these examples is that, for companies that design and market products capable of collecting, storing, accessing or transmitting personal information, it is enormously helpful to include a meaningful layer of review early on in product design (or modifications of product design) with an eye toward privacy. This type of product review could evaluate the intended and potential data flows and access through the product, and whether the existing settings and capabilities sufficiently protect the data.

The review also could evaluate whether these data flows are consistent with product representations and permission settings about how personal information is handled and shared (including any promises made in privacy policies, user interfaces and product user guides about personal data flows), and whether such data flows and data handling are consistent with legal requirements, and requirements from business partners and applicable industry standards.

This type of review might result in recommended changes to what personal information is collected, what settings are applied to such data collection or access, or what disclosures and consent mechanisms are employed. While this type of review can delay product launch and require some negotiation with product designers, if the privacy review does not occur, then the resulting product design is left to chance with respect to compliance with privacy laws. That might have been a lower risk years ago, but in today's environment, this may be a key factor in a product's success or failure.

Considerations From the User Experience

It is understandable for companies to be confused about what exactly are the privacy requirements to a given product or service, particularly given how the law in this area continues to evolve. But many compliance decisions are firmly rooted in evaluating information collection, sharing and communication from the user experience, and placing a premium on developing trust with end users. For example, consideration of whether the information collection or use would be so (negatively) surprising to the consumer if known can help issue spot and prevent a privacy problem. What would a typical consumer expect regarding the personal information the product will collect, and how that personal information will be used?

In this way, technology benefits and social science are worth considering together. If there is a disconnect from a user experience between what and how a company is communicating these points, that disconnect potentially threatens the company's brand and trust with end users (and with business partners who may not wish to do business with a company that is negatively stigmatized over a privacy mishap). It's not simply a matter of doing the right thing; a company's success can ultimately depend on sensitivity to an appropriate privacy approach.

Conclusion

While there may be uncertainty about the exact contours in privacy law, it is clear that the FTC will continue to closely scrutinize companies' practices with respect to the handling and security of personal information. This scrutiny is even more focused in the mobile business sector in which the FTC has, on a monthly basis, announced some type of mobile development — from mobile-related business guidance, to the most recent enforcement example, to more workshops, including a forthcoming forum to evaluate threats to mobile devices. That focus is likely to continue and remain a high priority for the commission for the foreseeable future, and similar measures are likely to be reflected in consumer class actions and state regulatory actions. For these reasons, companies would be wise to allocate sufficient resources to ensure that privacy is meaningfully addressed in business practices and policies.

--By Alysa Zeltzer Hutnik, Dana B. Rosenfeld and Christopher M. Loeffler, Kelley Drye & Warren LLP

Alysa Hutnik and Dana Rosenfeld are partners and Christopher Loeffler is an associate in Kelley Drye's

Washington, D.C., office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Defined as information from or about an individual consumer collected by a company through a covered device or input into, stored on, captured with, or transmitted through a covered device, including but not limited to (1) a first and last name; (2) a home or other physical address, including street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other state-issued identification number; (7) a financial institution account number; (8) credit or debit card information; (9) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol address, a mobile device ID, or processor serial number; (10) precise geolocation data of an individual or mobile device, including GPS-based, Wi-Fi-based, or cell-based location information; (11) an authentication credential, such as a username and password; or (12) any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, emails, text messages, photos, videos, and audio recordings.