FTC Settles with Device Manufacturer HTC America over Charges that HTC Products Had Security Design Flaws

In taking action against HTC America, a mobile device manufacturer, last week for alleged data security design flaws in its devices, the U.S. Federal Trade Commission demonstrated a broad view of the scope of its authority under the Federal Trade Commission Act to regulate data privacy and security principles, which all providers of consumer applications and devices should note. On February 22, the FTC announced a proposed settlement with HTC America over alleged claims that the company had committed unfair trade practices by failing to employ reasonable and appropriate security practices in installing software on its smartphones and tablets that had security vulnerabilities. The FTC claimed in its complaint that these security vulnerabilities were unfair trade acts or practices because they provided a gateway through which consumers might be harmed that was neither avoidable by consumers nor offset by countervailing benefits to customers or competition. The FTC also brought a deceptive trade practices claim based on statements in HTC's product manuals and mobile device interfaces.

The proposed settlement with HTC America reflects the increased focus the FTC has placed on pushing all actors in the electronics and software supply channels – whether upstream product manufacturers or app providers – to incorporate "privacy by design" principles in the product designs. The action should be of concern to a wide range of parties operating in those channels, even if they themselves do not collect or process consumer data but merely provide tools for doing so.

The FTC's complaint does not explicitly allege that any act or omission by HTC America itself caused an immediate loss or breach of consumer data. Rather, the agency alleged that tools HTC America had installed on its Android devices caused consumer harm because they made it possible for malicious applications to possibly later be added to the devices that would take advantage of the security vulnerabilities in the HTC America tools. According to the complaint, HTC America's security design choices made it trivial for malicious apps to access the devices' microphone (allowing surreptitious recordings), text messages, digits dialed, web and media history, email addresses, phone numbers, and GPS location data. This information could be used by hostile third parties, the FTC asserted, to harm consumer victims physically, through identity theft or by using their device in fraudulent text messaging schemes.

Such security flaws were difficult for consumers to avoid, the FTC claimed, but allegedly could have been avoided by HTC America had it "implemented readily-available, low-cost measures to address these vulnerabilities," such as common permission check code when programming pre-installed applications or logging tools. Because HTC America's security flaws allegedly enabled substantial injury to consumers without a countervailing benefit, the FTC claimed that they constituted an unfair act or practice. Further, the FTC alleged HTC America had deceived consumers through statements in its user manuals and mobile device interfaces that expressly or implicitly suggested to consumers that their data would not be disclosed to third parties absent express consumer permission, which the alleged vulnerabilities allowed third-party applications to bypass.

HTC America agreed to enter into a settlement that includes a consent order requiring HTC America to, among other things, implement a comprehensive security program, develop security patches to fix the identified security vulnerabilities, and obtain initial and biennial security assessments. The consent order, including its audit provisions, would remain in effect for 20 years. The proposed consent order is also notable for applying to any electronic products developed by HTC America or its affiliates, and for defining a broad set of data as among the personal information that HTC America is to protect, including names, addresses, screen names, authentication credentials, cookies and phone numbers.

ATTORNEY ADVERTISING

The FTC had foreshadowed this enforcement action in some of its recent public statements regarding privacy, in which the FTC signaled that its focus is broader than data brokers and others who collect and handle consumer data. For example, in a 2012 report suggesting best practices for data privacy and security, the FTC asserted its framework applies to nearly all companies "that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device." This proceeding against HTC America follows other recent agency activities aimed at regulating the security and use of consumer data, including efforts to improve mobile privacy disclosures, an overhaul of the Child Online Privacy Protection Act, and several actions against software developers for failing to adequately protect customer data aimed at a wider set of actors.

The FTC's action against HTC America, its first privacy action against a device manufacturer, and its aggressive stance that security design vulnerabilities can constitute "unfair" trade practices, has significant ramifications for parties that may not have traditionally considered themselves within the scope of data privacy laws. Electronic hardware manufacturers, software providers, and other parties that allow or help users to store or transmit their data should review their existing security design and data processing policies and practices in light of this settlement.

For more information regarding the HTC America settlement and its potential impact on your operations, please contact a member of our leading privacy and data security team, including Jim DeGraw, David McIntosh, Doug Meal, and Mark Szpak.

ropesgray.com

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have. © 2013 Ropes & Gray LLP

ATTORNEY ADVERTISING