A Quick Overview of Hot Topics in Privacy Law

April 2013

It has been a busy late winter for privacy law. Here are a few recent developments that may have significant long run implications.

Be Careful What You Say Everywhere

On February 22, the Federal Trade Commission (FTC) announced that it had entered into a consent decree with HTC America, the device manufacturer, for allegedly misleading statements regarding the security of the HTC version of the Android operating system, which it deemed an unfair trade practice.

What is interesting about this case is that nowhere in the FTC's complaint does the term “privacy policy” appear. Instead, the FTC based its complaint not on alleged misstatements or omissions in the company's privacy policy—the source typically relied upon by the FTC in bringing a deceptive practices privacy or security claim—but on misstatements in the owner's manual that accompanied the device and in its error reporting tool that the company made available to customers.

The takeaway is that a company must make sure that all of its representations regarding privacy and security are accurate, not merely those presented in the formal “privacy policy.”

Are You Ready for the Expanded COPPA Regulation to Take Effect on July 1?

The FTC's expanded regulation to implement the Children's Online Privacy Protection Act (COPPA) will take effect on July 1. As reported in our January issue, the agency in December revised its decade-old rule to expand the applicability of COPPA to mobile devices and to many advertising networks. The new regulation also increases the circumstances in which websites and applications could run afoul of the rules.

The bottom line is that COPPA will apply to, and impose many obligations on, online services beyond those one normally would think of as being directed to children, while retaining the law's strict liability standard. Websites and mobile applications have only a little time in which to review their operations to determine whether they are in compliance.

Possibly the most significant revisions to the regulation are (1) the extension of its applicability to third-party services, such as plug-ins and advertising networks having knowledge that a website they serve is directed to children under the age of 13; and (2) applying it to mobile applications. In addition, by expanding the definition of “online contact information” to include screen names that function as contact addresses and that of “personal information” to include photographs, videos or audio files containing a child's image or voice, the FTC's revised rule will apply to much more user-generated content than before.
The amended FTC regulation also imposes new “just in time” parental notice requirements, and creates a new duty to secure children's personal information, to conduct due diligence before disclosing such information to third parties and to delete such information after it is no longer “reasonably necessary.”

All businesses operating online should review their practices in light of the new Rule. With the amendments, COPPA will cast a much wider net, reaching companies that may not consider themselves to be interacting online with children. And you can expect the FTC to enforce COPPA actively, imposing monetary penalties and reputational risks.

Websites, apps and online services must act swiftly to ensure that they will be in compliance with the new rules by July 1. Recommended actions include (1) reviewing a site's (or an app's) existing operations to assess the implications of the new regulation; (2) clarifying the relationships among website and third-party services, including advertising networks and plug-ins; and (3) revising their privacy policies and practices as appropriate.

ECPA Reform Is Gearing Up

After several years of being urged to do so by industry and privacy advocates, Congress has begun to consider updating the Electronic Communications Privacy Act (ECPA) (which predates the Internet as we know it) to reflect the ubiquitous nature of email, social media, smartphones and mobile services.

One of the biggest issues concerns the legal standard that law enforcement must satisfy in order to access the contents of email. Current law, which dates from 1986, requires a showing of probable cause before law enforcement can obtain the contents of emails held in storage for less than 180 days, but law enforcement can obtain the contents of older emails upon showing merely that the contents may reasonably relate to an ongoing investigation. This distinction dates from an era before retention of emails in web-based email systems became commonplace, and the distinction has been difficult to justify for a number of years. Microsoft recently announced that it provided U.S. law enforcement with the contents of more than 1,500 communications in 2012, although some of those were pursuant to a warrant.

Several members of Congress have proposed amending the law to require that law enforcement demonstrate probable cause before obtaining the contents of an electronic communication, such as an email. This is consistent with the United States Court of Appeals for the Sixth Circuit's holding in U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2012), that the provisions of ECPA allowing law enforcement to obtain the contents of emails by means of a subpoena or court order based on less than probable cause are unconstitutional. The bill, S. 607 (sponsored by Sen. Patrick Leahy D-VT), would eliminate the 180-day rule.

The Department of Justice testified before a House of Representatives Judiciary subcommittee that the 180-day rule has likely outlived its appropriateness, but urged that any new legislation still provide some means by which investigators may obtain the content of emails short of a probable cause showing. It did not explain just what that might be.