Proskauer

A Moment of Privacy

December 2011

And now for the question:

Q: Do I really have to obtain consent from all my customers to make a change to my privacy policy? No one else seems to be following that rule.

A: We get this question all the time. It is understandable, given that we often watch Web-based companies expand their usage of consumer data without the affirmative consent of their users. (In other words, they add a new offering to their service that expands their use or sharing of consumer data, and they default their users into the new offering.) Sometimes they back off temporarily when faced with media backlash or Congressional or regulatory scrutiny, but the pattern nonetheless persists in the long term. Sometimes we scratch our heads in wonder, since the FTC has taken the position in countless actions for over a decade that if you make a material, adverse, retroactive change to your privacy policy, you need to obtain consent from consumers to apply your new policy to the data you collected under your old policy.

Last week, the FTC gave us their latest message. This time, it took the form of a settlement with Facebook in an action alleging that Facebook engaged in unfair and deceptive trade practices by, among other things, altering or enhancing their service in a manner that expanded their sharing of user data, without obtaining the consent of their users. (See our recent blog post detailing the settlement in full.)

In Facebook's defense, they actually did, at least in some instances, take steps to obtain the consent of their users by requiring users to click through a multipage Privacy Wizard that walked users through the revised privacy settings. However, the FTC alleged that the Privacy Wizard process was in itself deceptive, since the explanatory wording used on the Wizard spun the changes as affording more control on the part of users, when in fact, according to the FTC, the changes reduced user control over how their data would be shared with third parties and overrode users' existing privacy settings.

Under the terms of Facebook's settlement with the FTC, Facebook denied all the FTC's legal and factual allegations (with the exception of those regarding jurisdiction), so an outsider's only way of knowing the facts at hand is through his experience as an observant user of Facebook over the course of years, or, alternatively, trust in the accuracy of media coverage of Facebook's privacy changes over the last several years.

It is worth noting that Facebook is not required to pay a fine under the settlement. However, as part of the settlement, Facebook is required to suffer the scrutiny of the FTC for the next twenty years. For example, as is characteristic of the FTC's privacy settlements, Facebook must retain an independent third party to assess and report on its privacy practices biennially. It also must implement a privacy program that entails taking a "privacy-by-design" approach to its product development going forward, and it must retain for the FTC's review: (i) all widely disseminated materials relating to its privacy practices and changes thereto, including any backup materials, for the next three years; (ii) all consumer complaints for six months after receipt; (iii) all documents prepared by or on behalf of Facebook that contradict, qualify or call into question its compliance with the settlement terms for five years from receipt thereof; (iv) documentation of changes that Facebook makes to its privacy policies along with documentation of users' consent and their settings prior to consent for three years from the date of such documents' preparation or dissemination; and (v) all backup materials of its biennial privacy assessments for three years after each such assessment.

What is the takeaway for other businesses? One, the FTC wants businesses to disclose important changes in their privacy practices (such as how they share data with third parties) conspicuously, and not merely in their privacy policies and other legal boilerplate. Two, the FTC wants businesses to obtain affirmative consent from their customers when they make material adverse retroactive changes to their privacy policies. (They can obtain user consent the next time the user interacts with the business, such as when the user returns to the business's Web site.) Three, the FTC wants businesses to be upfront and straight with their customers when they solicit their consent to new uses they want to make of user data – not to "spin" changes that expand the business's usage rights as if they are enhancing user privacy.

It is worth noting that the statute that the FTC invokes to set these standards (the FTC Act) does not contain any of these requirements. It simply prohibits unfair and deceptive trade practices. Yet, each time we see an example of the FTC's enforcement of this law in the privacy space, we learn something about the FTC's interpretation of the law. (It is not often challenged, although it could be by a defendant so inclined.) And anything new and interesting we learn from these settlements is what we at Proskauer impart to you.

Have a question? Email Kristen J. Mathews at kmathews@proskauer.com.