March 14, 2014

NTIA Code of Conduct for Mobile App Notices: Let Transparency Be Your Guide

The National Telecommunications and Information Administration (NTIA) announced a voluntary Code of Conduct for mobile application ("app") short notices, (Code of Conduct) developed through the Multi-Stakeholder Process on Application Transparency convened by the U.S. Department of Commerce in June 2013. The purpose of the short form notices is to provide consumers enhanced transparency about the data collection and sharing practices of apps that consumers use. See http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

The Code of Conduct provides that app developers and publishers that voluntarily elect to enhance transparency by adopting a short form notice should describe in the notice

a) "the collection of types of data collected" (see the list of data categories below), and "whether or not consumers know that it is being collected";

b) "a means of accessing a long form privacy policy, if any exists";

c) "the sharing of user-specific data, if any, with third parties" (see the list of third-parties below); and

d) "the identity of the entity providing the app."

The Code of Conduct requires that "short form notices" convey the required information to app users in "a consistent manner that is easy for consumers to read and understand."

In particular, the short form notice should clearly disclose collection of the following data categories:

- Biometrics (information about the user's body, including fingerprints, facial recognition, signature and/or voiceprint)
- Browser History (a list of websites visited)
- Phone or Text Log (a list of the calls or texts made or received)
- Contacts (including a list of contacts and social networking connections, and their phone numbers and postal, e-mail and text addresses)
- Financial Info (includes credit-, bank- and consumer-specific financial information such as transaction data)

- Health, Medical or Therapy Info (including health claims and other information used to ensure health or wellness)
- Location (precise past or current location of where a user has gone)
- User Files (files stored on the device that contain a user's content, such as calendar, photos, text or video)

Further, the short form notice should state whether the app shares user-specific data with any of the following categories of third-party entities:

- Ad Networks (companies that display ads to the user through apps)
- Carriers (companies that provide mobile connections)
- Consumer Data Resellers (companies that sell consumer information to other companies for multiple purposes, including offering products and services that may interest the user)
- Data Analytics Providers (companies that collect and analyze the user's data)
- Government Entities (any sharing with the government except where required by law or expressly permitted in an emergency)
- Operating Systems and Platforms (software companies that power devices and app stores and companies that provide common tools and information about app consumers)
- Other Apps (other apps of companies that the consumer may not have a relationship with)
- Social Networks (companies that connect individuals around common interests and facilitate sharing)

At the beginning of March, software developer Intuit Inc. announced it would soon release an open source code that will allow mobile app developers to craft short privacy notices that comply with the NTIA proposed voluntary short form notice provisions. The code will provide a customizable template that developers can use to develop a privacy notice that will incorporate all of the elements described above. This announcement comes a week after Lookout Mobile Security released its own open-source mobile app privacy notice code for developers.

These open source code modules should encourage mobile app developers to voluntarily comply with the Code of Conduct endorsed by the NTIA working group before it becomes the law of the land.

Day Pitney recommends that all app developers take a close look at the templates, given the legal exposure they could face for inadequate disclosures. No laws prohibit the collection of sensitive information from consumers using mobile apps, so long as you tell the consumer what you are doing. By adopting templates promulgated under the guidelines of the Code of Conduct, you can reduce the risk of becoming a target of the Federal Trade Commission, a state attorney general or the private plaintiffs' bar.