THE
NATIONAL LAW REVIEW

Privacy and Data Security Reminders for Mobile Technology Providers

Article By
Ed Chansky
Erica Okerberg
Greenberg Traurig, LLP
Alerts

- Consumer Protection
- Communications, Media & Internet
- Administrative & Regulatory

- All Federal

Tuesday, September 16, 2014

Greenberg Traurig, LLP recently hosted a talk in its Silicon Valley office about privacy and software security for mobile technology providers with Nithan Sannappa, an attorney in the FTC's Division of Privacy and Identity Protection. Three key areas were highlighted.

Adopt Privacy by Design

Privacy by Design is a central principle the FTC and other regulatory bodies strongly recommend for mobile technology. There are seven foundational principles underlying Privacy by Design:

1. **Be proactive** - Seek to anticipate and prevent issues, don't wait to address those that arise.

2. **Make privacy the default** - Allow consumers to choose to share their data.

3. **Embed privacy into the design** - Create software or apps based on privacy considerations.

4. **Offer the full package** - Don't ask users to trade functionality for privacy and/or security.

5. **Provide start-to-finish privacy** - Implement and maintain privacy and security.

6. **Be transparent** - Make security and privacy practices visible to consumers and providers.

7. **Focus on users** - Give users the control to choose how their data is used and protected.

Sannappa reiterated the FTC's support of Privacy by Design and also emphasized the following considerations:

- **Type of data** - Collect only what you need.

- **Retention** - Store data only for as long as you need.

- **Announce practices** - Disclose privacy terms in simple language. Consider putting key items at the point when triggered (just-in-time disclosure), such as when a user is downloading an app, rather than just in a formal privacy policy.

- **Geolocation and other sensitive data** - Be particularly careful and transparent about unexpected practices or collection of sensitive information. For example, if your app will gain access to a user's complete address book, geolocation information or other personal data, these facts should be disclosed clearly and conspicuously, and at a relevant time to alert the user prior to installing the app. The consumer should always have appropriate notice and choice over such practices.

- **Adequate security** - Your software should store and transmit data securely. Remember that mobile devices are prone to loss and theft, and they often connect to unsecured networks. Design software to store and transmit data securely with these types of factors in mind.

Review your Privacy Policy

A proper privacy policy puts consumers on notice of the data collection and sharing practices of the relevant website or app. Key considerations include the following:

- **Keep it simple** - Write your policy in terms a reasonable consumer can understand.

- **Just-in-time disclosure** - Consider where your policy is located. It is a good idea to reiterate key terms when triggered, such as the point when an app is downloaded or installed.

- **Make sure it's true** - Don't make any unsupported privacy or security guarantees. Make sure your privacy policy accurately describes your practices.

- **Keep it current** - Review your privacy policy and privacy-related statements regularly to make sure they conform to any changes in your practices, technology or consumer expectations.

Tips to Help Avoid Security Traps

By taking a few common-sense precautions, companies can be better equipped to identify and resolve security issues when developing and deploying mobile technologies. Some highlighted tips include:

- **Put someone in charge of security during development** - This person should have the skills to design/create a secure environment for collecting and storing data. Keep this person involved even after the software/app is deployed to help deal with any later-discovered issues.

- **Read developer documentation** - If you use an outside developer, have a qualified member of your team review the security-related information the developer provides. Ultimately, you are responsible for how your software/app works and for any consumer complaints.

- **Pay attention to industry guidance** - Adopt best practices suggested by applicable industry groups to take advantage of their collective knowledge and insights. Examples include CTIA, GSMA and DAA, which have adopted various self-regulatory guidelines on topics such as geolocation data, behavioral advertising tracking and more.

- **Pay attention to industry-specific laws** - Financial services, health care and children all are subject to special laws. For example, if a child-oriented app gathers geolocation information, the FTC considers such information personal and requires parental consent before such information can be gathered about a child under age 13.

- **Remember that security is an ongoing process** - Security threats are ever-changing. Monitor developments in the marketplace and continually update the security of your software or app after its launch to help stay current with new issues and threats as they arise.

- **Keep your ears open** - Establish a process to receive feedback from researchers and users and pay attention to that feedback.

- **Encrypt sensitive data** - All data that may be considered sensitive should be encrypted. Examples may include, among other things, credit card numbers, Social Security numbers, health records, financial records and information about children. The level of encryption will depend upon the sensitivity of the data, the potential threats to security of that information and, in some cases, laws governing particular industries such as finance and health care.

- **Grant access only on a need-to-know basis** - Consider why you are collecting certain data. Then, determine who needs access to that data to reach your goals. Limit access only to those people.

Privacy and data security continue to be hot-button issues for federal and state regulators. Private class action litigation in this area is also growing. To help minimize risks, companies developing mobile technologies are well-advised to scrutinize their data-gathering and data-security practices, harmonize their

published privacy policies with those practices, and remain vigilant in a fast-changing marketplace.

Source URL: https://www.natlawreview.com/article/privacy-and-data-security-reminders-mobile-technology-providers