Global Data Privacy and Security Team

Mobile App Privacy Policies

Many of the most popular mobile apps collect personally identifiable information. Although most app developers are not required to display a privacy policy under federal law, they are contractually required to do so pursuant to the terms and conditions of the platform for which the app will be marketed. In addition, the California Attorney General has indicated its belief that applications that collect personal information are required to post a privacy policy pursuant to the California Online Privacy Protection Act.

Possible penalty under California law for each app downloaded without a privacy policy.[1]	Percentage of mobile apps that collect private information but do not have adequate security in place to protect it.[2]	Mobile apps do not use proper encryption techniques when storing data on mobile devices.[3]
$2,500	**86%**	**75%**

Consider the following privacy issues when developing a mobile app:

- ✓ **Does the app have a privacy policy?** Privacy policies are a best practice if the app will be used in connection with personally identifiable information.
- ✓ **Is the app directed to users younger than 13?** Under the Children's Online Privacy Protection Act, the Federal Trade Commission regulates the collection of information from children under 13.
- ✓ **How is personally identifiable information stored by the app?** Apps can store data in multiple places, including the device, backups of the device, and the app provider's servers. A best practice is for the mobile app privacy policy to state accurately where the personally identifiable information is stored.
- ✓ **Using the app, does the user communicate personally identifiable information to others?** A useful privacy policy accurately states whether the data that the user provides is relayed to anyone else.
- ✓ **Does the mobile app provider securely communicate any personally identifiable information?** A 2013 study concluded that 18 percent of apps sent usernames and passwords by non-encrypted communications and other apps failed to implement secure communications properly. A privacy policy should state whether the app transmits personally identifiable information, and, if so, whether the information is encrypted in transit.
- ✓ **If the app crashes, would diagnostic data about the crash include personally identifiable information?** Some apps do not transmit personally identifiable information in their normal operation, but diagnostic data may inadvertently capture such information in an unencrypted manner.
- ✓ **Can the presence of the app be used by others, such as websites or other apps, to identify the user?** Some websites and even other apps may determine that an app is present on a mobile device.
- ✓ **Can access to the app be revoked remotely?** The revocation of access to an app potentially raises privacy concerns that may need to be addressed in a privacy policy.
- ✓ **Is an adequate system in place to notify users of a data breach involving personally identifiable or confidential information?** A best practice is to implement a notification procedure in the event servers containing personally identifiable information collected through the app are breached.

[1] http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance
[2] http://www8.hp.com/us/en/hp-news/press-release.html?id=1528865#.VaRAHl9VhBc (study conducted in 2013).
[3] http://www8.hp.com/us/en/hp-news/press-release.html?id=1528865#.VaRAHl9VhBc (study conducted in 2013).

For more information on state data breach notification laws or to subscribe to the Bryan Cave Breach Notification Survey contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6000

John C. Bush
Associate
john.bush@bryancave.com
One Atlantic Center, 14th Floor
1201 W. Peachtree St., N.W.
Atlanta, GA 30309-3471
phone: 404 572 6600

BRYAN CAVE