MOBILE APPS

New Risks and How to Address Them

As companies continue to reach out to customers and the public using new technologies and platforms, many of them are providing mobile applications (apps) for smartphones and other devices. Keeping customers and others as engaged and interested as possible is essential for most businesses, and mobile apps can be an excellent tool. However, as is all too often the case, innovation includes potential and actual risks.

As the number and variety of mobile apps has expanded dramatically, the plaintiffs’ class action bar, state and federal regulators, and the media have focused their attention more and more closely on data privacy and security.

- **Increased class action risk.** Plaintiffs have sued developers and companies that publish, own or distribute mobile apps in class action suits based on alleged misrepresentations about the collection and use of data. They have alleged, for example, that collecting and using certain end-user information (e.g., contacts and app usage history) without sufficient notice and choice violates state and federal privacy laws.

- **Increased state regulatory activity.** For example, the California attorney general announced that all app developers that collect personal information from California residents must have a privacy policy in compliance with California’s Online Privacy Protection Act. She also reached agreement with the major platform providers concerning mobile app requirements. The New Jersey attorney general sued 24x7 Digital because the company’s mobile apps sent unique hardware identifiers and the first and last names of end-users to a mobile analytics company. Other states are likely to jump on the bandwagon.

- **Increased federal regulatory attention.** The Federal Trade Commission’s Final FTC Privacy Report indicates that consumer data that can be reasonably linked to a specific consumer, computer or other device is subject to protection under its privacy framework. This means that IP addresses, device identifiers and randomly assigned user IDs are not “anonymous,” and if collected or shared by companies without appropriate disclosure, transparency and control, may trigger an FTC investigation or enforcement action. The FTC is focused on mobile apps and has been highly critical of the industry. In addition, FTC lawyers have stated that investigations of misrepresentations in the mobile app area are underway and will be the subject of increased attention. Companies that don’t pay attention to their apps run the risk of an FTC inquiry or other action.

RISK PROTECTION

As a result of the attention being paid to mobile apps, Holland & Knight’s Data Privacy and Security Team offers clients services to help them protect themselves from these emerging risks, including the following:

**Network traffic analysis.** Our team conducts a “black box” review of a mobile app using network analyzers, proxy tools, and, for certain platforms, reverse engineering software. The aim is to identify the categories of information...
collected from the end-users of the app, the existence of first-party and third-party tracking mechanisms, and the identity of third-parties receiving information about the end-user as a result of the end-user’s use of the mobile app. After conducting this technical review, we provide recommendations regarding the choice and control options and mechanisms within the mobile app and advice regarding data retention and security measures. We perform this analysis on Apple iOS, Android and other platforms.

Review of local storage. An important aspect of analyzing the privacy characteristics of a mobile app is to isolate what is stored and tracked locally for subsequent transmission over the network. Although this is more difficult with mobile devices than with traditional desktop machines, it is another level of analysis provided by our team.

Privacy threat model. With a company’s specific legal and regulatory context in mind, we provide a holistic view of relevant areas of potential data leakage in the context of mobile apps. A company can use a privacy threat model as an aid to future app development and compliance efforts.

Analysis and advice regarding disclosures. Our team reviews current disclosures relating to transparency, choice and control pertaining to the app environment. We identify what disclosures are currently being made with respect to what personal information is being collected or accessed, who is collecting and using personal information, why the personal information is being used, what personal information is being shared, and with whom and for what purposes. Following the technical and legal review, we offer advice regarding the deployment, presentation and content of privacy policies and other relevant disclosures.

Analysis of third-party privacy controls. Our team collects and reviews all relevant vendor and third-party agreements (including passive agreements that are disclosed in any relevant Application Programming Interface, or API) and provides recommended changes, revisions and amendments to those agreements.

SCOPE OF OUR WORK

Our work is typically broken down into three parts. We have developed a substantial body of knowledge about the technical and business practices of the third-parties that are often implicated in mobile app network traffic (e.g., ad delivery networks, analytics companies and push notification vendors). As a result, we have developed economies of scale for conducting tech reviews and for providing advice on disclosures, choice options and transparency.

Part 1

We conduct a privacy audit and an analysis of network traffic within the mobile app’s environment. This includes a thorough review of current disclosures relating to transparency, choice and control; determining the context of the mobile app; identifying the data elements relating to the end-user’s use of the mobile app; conducting a “black box” review of the mobile app to identify, among other things, the categories of information collected by the end-user and the existence of first- and third-party tracking mechanisms; identifying the categories of information that the client shares with others, including third-parties, vendors and content providers; and collecting and reviewing vendor and third-party agreements disclosed in any relevant Application Programming Interface (API).
Part 2
Drawing on our privacy audit and analysis of network traffic, **we perform a risk analysis** based on existing legal requirements, actual and proposed/imminent regulatory frameworks, best practices and Mobile App Market Company obligations/requirements. We then identify non-compliance items based on that risk analysis and exposure to potential privacy class action claims, if any, based on the current and anticipated litigation landscape. We also identify potential areas of criticism from regulators, privacy researchers and the press.

Part 3
**We provide recommendations** regarding the deployment, presentation and content of privacy policies and other disclosures; choice and control options and mechanisms within mobile apps; data retention and security measures; addition or subtraction of mobile app features to manage your risk profile; Standard Operating Procedures for use internally of instructions for third-parties in regard to mobile app development and deployment; suggested revisions to existing contracts; and templates for future third-party agreements.

**CONTACT OUR TEAM**

**Chris Cwalina**  
Partner  
202.469.5230  
chris.cwalina@hklaw.com

**Steve Roosa**  
Partner  
212.513.3544  
steve.roosa@hklaw.com

**Ieuan Mahony**  
Partner  
617.573.5835  
ieuan.mahony@hklaw.com

**Shannon Hartsfield Salimone**  
Partner  
850.425.5642  
904.798.7331  
shannon.salimone@hklaw.com

Co-Chairs  
Holland & Knight Data Privacy and Security Team