Mobile App Privacy: The Hidden Risks

Christopher G. Cwalina, Richard Raysman and Steven B. Roosa, Holland & Knight LLP with PLC Intellectual Property & Technology

A Practice Note discussing privacy considerations in the context of mobile applications (apps), including liability risks associated with mobile app information collection and practices for addressing those risks. This Note provides an overview of how mobile apps use technology to collect information about and track end users, identifying key differences between mobile apps and websites in terms of how they collect and store end-user information and end users' ability to control that collection and storage. It also discusses the legal framework governing mobile app privacy, including FTC rulemaking, guidance and enforcement actions.

Privacy is among the key legal risks associated with mobile application (app) development and deployment. These risks arise, in particular, because:

- Mobile apps collect user information in new ways that often are not understood or capable of being controlled by the average end user.
- The smaller screen size of many mobile devices can make it harder for an app to communicate user information practices to end users.
- Apps are increasingly under the scrutiny of regulators and advocacy groups, who use independent researchers to identify undisclosed user information collection and sharing.

To properly manage these risks, legal counsel must be involved throughout the process from the early stages of development and continuing after the app has been launched. This includes actively monitoring:

- Cutting edge forms of marketing and advertising.
- The background collection and sharing of end user information.
- The content and mode of presenting consumer disclosures.

This Note focuses on the privacy issues associated with mobile apps. In contrast, a number of mobile browsers and related privacy controls have evolved to operate similarly to their PC-based counterparts. Specifically, this Note examines issues regarding:

- Mobile app information collection and retention.
- The legal exposure and risks associated with mobile app privacy concerns.
- Children's online privacy and apps.
- Achieving compliance and reducing risk.

MOBILE APP INFORMATION COLLECTION

Understanding the technical ways mobile apps collect and share information is key to identifying and managing the regulatory and litigation risks associated with mobile app privacy.

Counseling in this area requires familiarity with the:

- Types of information apps must collect and share (*see Necessary Information Collection and Storage*).
- Ways mobile app technology collects and shares information (see *Mobile App Tracking Technology*).

Website Privacy Legacy

A major challenge for managing mobile app privacy risk is that ideas about online privacy and security gained prominence as the internet evolved as a mainstream communication platform, and common understandings about online privacy remain grounded in the website model. However, mobile apps differ from websites in certain critical ways:

- How they collect, store and use user information.
- The types of user information they can collect and use.

In particular, key privacy-related differences between websites and mobile apps include that:

- Apps collect, store, use and share end user information in ways different from browser software and, therefore, can often surprise even web-savvy end users. This occurs at a technical level of mobile device's operations that is invisible to the average end user.

- While end users have ways to avoid most browser-based tracking with a small amount of effort, mobile apps frequently use hardware device identifiers (hardware IDs) that cannot be deleted or reset. For more on browser-based information collection and storage, see *Box, Website Information Collection*.

Necessary Information Collection and Storage

Recognizing and educating end users that certain information collection and retention is necessary for an app, like websites, to provide a satisfactory user experience is critical to managing privacy risks. Many mobile app functions either require or are enhanced if the servers remember certain facts about an end user. This information may include, for example, the user's:

- Identity.
- Usage history.
- Past log-ins.
- Navigation.

This remembering is critical for both app providers and third parties who provide services to them, for example, to:

- Enable certain functionality, for example, shopping carts.
- Customize content based on the user's preferences.
- Provide a secure environment.
- Serve targeted advertising.
- Analyze usage (analytics), which can be used to improve the app or its features.

However, it also presents a privacy trade-off. The more an app or service provider knows about a particular end user and his usage, the better it can tailor certain features for a better user experience. However, it also increases the risks that the information will be leaked or misused.

Decentralized Information Collection

Many mobile apps, like websites, use third parties to:

- Serve ads.
- Perform analytics.
- Deliver content.

As with websites, when an end user downloads or uses an app, parties in addition to the app publisher are likely collecting information about that user.

However, because apps are not browser-based (see *Box, Website Information Collection: Browser-based Privacy Framework*), there are no browser cookies available to allow third parties to remember end users across mobile apps in the way that third parties remember website users across large portions of the web. Therefore, in contrast with the website model, mobile app information collection is decentralized and controlled by the app itself in an isolated environment. In instances where apps use browser functionality, the browser and the app functions generally operate separately at the technical level.

Mobile App Tracking Technology

To track end users, apps generally use one or more of the following:

- Hardware IDs (see *Hardware IDs*).
- Geolocation (see *Geolocation*).
- Metadata and information associated with other stored files, including photos, audio files, video and contacts (see Stored Files and Metadata).
- Information collected and stored in the app itself (see *App-specific Storage*).

As these practices have become more pervasive and provoked public backlash over data collection practices, some mobile software developers have begun to provide settings to enhance privacy. Therefore, some users, particularly those with new operating systems, may now have the means to control whether some apps may access location information or certain files on the device. However:

- Disallowing certain data collection may impair an app's usefulness (see *Necessary Information Collection and Storage*).
- Even with these privacy enhancements, most mobile app data collection remains beyond the end user's control.

Hardware IDs

Mobile app developers rely on hardware IDs to track end users and, in many cases, enable their apps' functionality. Hardware IDs also enable content and advertising providers to track end users across many mobile apps. Hardware IDs are unique permanent identification numbers or character strings associated with a device. Types of hardware IDs include:

- Cellphone radio (Mobile Equipment Identifier (MEID).
- International Mobile Station Equipment Identity (IMEI)).
- WiFi radio (Media Access Control (MAC)) address.
- Bluetooth radio identifier.
- Platform-specific identifiers, for example, Apple's Unique Device Identifier (UDID).

The key difference between hardware IDs and identifiers associated with website browser cookies is that hardware IDs are permanently associated with the device. By deleting cookies and local shared objects, an end user can typically prevent a certain amount of tracking and retain some degree of anonymity from third parties. Each time the third party's servers connect with the end user, the third party must set new, different, unique identifiers.

However, in the mobile app context, even if a user deletes the app, clears all web content, wipes all storage and restores factory defaults, the hardware ID remains unchanged. Third parties that have tracked the end user's network traffic and stored that information can still associate it with the end user's device. Therefore, a hardware ID can identify the mobile device for the life of the device. This has prompted objections from privacy advocates regarding the use of hardware IDs for tracking purposes.

Apple has taken some steps to address concerns that privacy advocates and others have raised about hardware IDs, including that it:

- Has created a software-generated identifier known as the Identifier for Advertising (IFA).
- Is expected to include in future versions of its mobile operating system a sliding toggle that will allow users to easily clear and reset the IFA.

Together, these would have a similar effect to deleting cookies in a browser.

However, UDIDs still exist on iOS devices, and many third parties continue to collect and use them to track users. The collection of end user MAC addresses also remains pervasive, as observed on both the iOS and Android platforms. Therefore, it is unclear whether:

- The IFA and similar measures will be widely embraced in the mobile app community.
- Even if they are embraced, developers and others will still collect hardware IDs alongside the IFA.
- Other mobile device and platform providers, notably Android, will take action to address hardware ID concerns.

Geolocation

Mobile apps also collect information about devices and end users through geolocation. Apps can collect location information using:

- Global positioning systems (GPS).
- Cell-tower proximity.
- WiFi hotspot locations.
- Internet protocol (IP) addresses.

Third-party code embedded in mobile apps may also collect geolocation information. App providers typically collect this information for:

- Analytics.
- Serving location-based targeted advertising.
- Geo-fencing, which is location awareness that prompts certain activity when a device enters or leaves a specified physical location. It also may be used for analytics related to physical places.

Stored Files and Metadata

Certain mobile apps also access various types of files stored on a mobile device, for example:

- Photographs.
- Audio and video clips.
- Personal contacts or other address book information.

This functionality may be included, for example, to enable users to:

- Share these items with others.
- Upload them to social networks or other websites.
- Connect with contacts, including for purposes of participating in games or interacting with them.

Some of these files may also contain metadata that can be used to identify, for example:

- When the file was created.
- Where the file was created.

App-specific Storage

For mobile apps as well as websites, user data can be stored remotely on servers on the web. A key distinction between mobile apps and websites, however, is that:

- In the website context, most user data that is stored locally is stored centrally in browser files.
- In the mobile-app context, information is stored locally by each app. Therefore, it is not centrally located, but is splintered and app-specific.

As observed using the forensic tools provided by Santoku Linux, app-specific, local storage may include special storage areas for third parties that the particular app uses for analytics or tracking ad-serving data. For example, ad-serving information stored locally may include:

- The device's UDID (see Hardware IDs).
- The number of ad impressions served.
- Timestamps for when ads were served.
- An identifier for ads served.
- Other unique identifiers and data.

Additionally, mobile apps generally do not provide tools for the average end user to:

- Examine local storage.
- Manage its contents.

The only control a user may have to control mobile app privacy may be to delete apps or doing a hard reset of app data. Some apps use app-specific cookies that, unlike browser cookies, cannot be accessed or deleted by the lay end user. The average end user typically does not even know that local, app-specific storage exists on mobile devices.

LEGAL EXPOSURE AND RISK

Mobile app privacy is generally subject to the same regulatory framework as website privacy. However, particularly because the mobile area is relatively new and still evolving, mobile app information practices are increasingly a focus of:

- Federal Trade Commission (FTC) investigations and rulemaking (see *FTC Regulation and Enforcements*).
- State legislative and enforcement action (see *State Regulation and Investigations*).
- Class action lawsuits (see *Consumer Class Action Suits*).

In addition, recent developments involving children's privacy online are relevant in, and in some cases prompted by the evolution of, the mobile app space (see *Children's Online Privacy and Apps*).

As mobile app regulation and enforcement continue at both the federal and state level, a developing patchwork of substantive laws and regulation is likely to make mobile app privacy compliance increasingly challenging.

For an overview of the laws governing consumer privacy in the US, see *Practice Note, US Privacy and Data Security Law: Overview* (www.practicallaw.com/6-501-4555).

FTC Regulation and Enforcements

At the federal level, the FTC regulates and enforces online (including mobile) privacy under Section 5 of the Federal Trade Commission Act (FTC Act), which prohibits unfair or deceptive acts and practices in commerce and empowers the FTC to enforce the Act (15 U.S.C. § 45(a)). The FTC has actively pursued mobile privacy on several fronts, including:

- Issuing guidance (see *FTC Privacy Report and Mobile Marketing Guidelines*).
- Enforcement actions (see *FTC Enforcement Actions*).
- Heightened focus on children's online privacy (see *Children's Online Privacy and Apps*).

FTC Privacy Report

In March of 2012, the FTC published its Final Commission Report (Report) on online and mobile privacy issues entitled *Protecting Consumer Privacy in an Era of Rapid Change*. The Report came during a period of increasingly aggressive enforcement by the FTC against technology companies, software companies and social networks. This trend appears to be encompassing traditionally non-tech companies as the focus shifts to mobile apps. In its Report, the FTC articulated its new "privacy framework," setting out best practices for companies that collect and use consumer data. The framework consists of:

- "Privacy by design" principles.
- Simplified consumer choice.
- Transparency regarding the collection and sharing of consumer data.
- The concept that consumers ought to have access to their sensitive data.

See *Legal Update, FTC Releases Final Consumer Privacy Report* (www.practicallaw.com/4-518-6623).)

Alongside the Report, the FTC:

- Announced plans to:
  - focus on the mobile industry; and
  - update its guidelines for mobile advertising practices.
- Called on companies to work toward improved privacy protections, including the development of short, meaningful disclosures.

Mobile Marketing Guidelines

Following the release of its Report, the FTC issued guidelines entitled *Marketing Your Mobile App: Get It Right from the Start*.

These guidelines are intended to help mobile app developers comply with truth-in-advertising and basic privacy principles when marketing new mobile apps. The FTC stressed that laws that apply to established businesses also apply to start-ups and app developers that are marketing and releasing new apps for consumers.

The guidelines apply to information both that:

- Users give to the developer.
- The software collects.

The general guidelines that the Report encourages app developers to consider include:

- **Truthful advertising.** The FTC cautions that an app developer should only make objective claims about an app that it can factually support. For example, claims that an app provides benefits related to health, safety or performance should be supported by competent and reliable scientific evidence.
- **Clear and conspicuous disclosures.** Any necessary disclosures about claims made should be clear and conspicuous. While the law does not dictate a specific font or type size, the guidelines note that the FTC has taken action against companies that have buried important terms and conditions, for example:
  - in long licensing agreements;
  - in dense blocks of legal language; or
  - behind vague hyperlinks.
- **Privacy by design.** The FTC suggests incorporating privacy protections into companies' everyday practices, including:
  - limiting the information it collects; and
  - providing consumer choice and opt-outs.
- **Privacy promises.** The FTC urges app developers to ensure they comply with their privacy policies, including:
  - employing practices consistent with assurances made to users about, for example, security standards and sharing information with advertisers; and
  - getting users' affirmative consent to material changes to information practices.
- **Data security.** The FTC also stressed the importance of data protection, noting that the law requires that they take reasonable steps to keep sensitive data secure. The FTC recommends as best practices that app developers:
  - collect only the information they need;
  - take reasonable precautions against well-known security risks;
  - provide access to information only on a need-to-know basis; and
  - safely dispose of information they no longer need

FTC Enforcement Actions

The FTC typically takes action where it believes a company misrepresents or fails to disclose either:

- Consumer information practices.
- Changes in those practices.

Misrepresentations that the FTC has focused on include, for example:

- Representing that third parties' access to end user information is more limited than it actually is.
- Representing that end users can restrict sharing of personal data when they cannot.
- Making untrue claims regarding security.
- Making untrue claims that information will not be shared with advertisers.
- Making untrue promises regarding the deletion of end user information.
- Falsely claiming that the company is in compliance with the *US-EU Safe Harbor Framework* (www.practicallaw.com/2-501-8616) for data transfers between the US and the European Union.

The FTC has also taken action against practices it considers inherently unfair, irrespective of whether they meet the threshold for being deceptive. For example, in FTC v. Frostwire LLC, the FTC sued the developer of a peer-to-peer file-sharing mobile app. The complaint alleged that the app's default settings were configured so that, immediately on a user's installing and setting up the app on a device, it would publicly share files stored on that device. According to the FTC complaint, the default settings were likely to cause consumers to unwittingly disclose personal files stored on their mobile devices. Among other things, the settlement:

- Bars the company from using default settings that share consumers' files.
- Requires the app to provide clear and prominent disclosures about file sharing and how to disable it.

(*FTC v. Frostwire LLC, No. 11-23643 (S.D. Fla. Stipulated Final Order Oct. 12, 2011).*)

State Regulation and Investigations

Some states, notably California, have also been aggressive in regulating and enforcing mobile app privacy.

California Online Privacy Protection Act

The California Online Privacy Protection Act requires that companies that collect personal information through websites or other "on-line services" post an accurate privacy disclosure that complies with the Act's requirements (*Cal. Bus. & Prof. Code § 22575-22579*).

California Attorney General Kamala Harris has interpreted "on-line service" to include mobile apps. On October 30, 2012, Attorney General Harris sent a letter to 100 companies that have mobile apps without privacy policies demanding that each conspicuously post its privacy policy in a means that is reasonably accessible to consumers. The letter gave recipients thirty days to comply, or otherwise face penalties of up to $2,500 per mobile application download. At present, the California Attorney General has commenced filing lawsuits against companies that are allegedly out of compliance.

California's potentially severe fines, which are assessed per download, are not limited to companies based in California. Instead, Attorney General Harris intends to reach well beyond the boundaries of her state to penalize any noncompliant company with mobile app users who are located in California. This effectively makes the California law reach around the globe.

Mobile Privacy Recommendations

On January 10, 2013, Attorney General Harris also released *Privacy on the Go: Recommendations for the Mobile Ecosystem*. The recommendations encourage app developers and other parties in the mobile industry to consider privacy at the outset of the design process. Specific suggestions include:

- Making a mobile app's general privacy policies easy to understand and readily available before a user downloads the app.
- Making readily available from within an app both:
  - a short privacy statement highlighting potentially unexpected practices; and
  - privacy controls that allow users to make, review and change their privacy choices
- Not collecting from users personally identifiable data that is unnecessary for an app's basic functionality.

(See *Legal Update, California AG Releases Privacy Recommendations for Mobile App Market* (www.practicallaw.com/9-523-5131).)

Other State Actions

Other states have also pursued mobile app privacy, including launching investigations pertaining to mobile apps based on various grounds. For example, in 2012, New Jersey filed, and then settled, a lawsuit against an app developer, 24x7 Digital LLC, for collecting personal information from children without parental consent. Other states, such as New York, have proceeded by way of informal inquiry.

Consumer Class Action Suits

An increasing number of consumer class action lawsuits alleging violations of end user's privacy rights are being brought against mobile app:

- Developers.
- Publishers.
- Platforms.

Like the website tracking suits that preceded them, the suits against entities in the mobile ecosystem typically assert multiple claims alleging violations of:

- The *Computer Fraud and Abuse Act* (www.practicallaw.com/2-508-3428) (CFAA).
- Federal and state wiretap statutes.
- State privacy and consumer protection laws.
- Unjust enrichment.
- Trespass.
- In some cases, the federal RICO statute.

While this area is relatively new and continues to evolve, several themes have emerged, including courts' willingness to:

- Apply general consumer protection laws to the mobile space (see Application of Consumer Protection Laws to Mobile Privacy).
- Take a broader view of justiciable harm in the mobile space than they have for websites (see Broader View of Justiciable Harm).

Application of Consumer Protection Laws to Mobile Privacy

Consumers claiming mobile-app privacy violations have had some success asserting rights under generally applicable consumer protection laws. In one case in District Court for the Northern District of California, the plaintiff end users claimed that Apple and certain app publishers violated their privacy rights under various federal and state laws by allowing the publishers' iPhone and iPad apps to collect personal consumer information. This included address book data, phone numbers, photographs, and geolocation information. The plaintiffs alleged that the publishers could then merge the information to discover the identity of, or de-anonymize, end users.

The court granted Apple's and the publisher's motions to dismiss the plaintiffs':

- CFAA and other federal claims based on the absence of economic harm.
- State law invasion of privacy claims, finding that a disclosure of such information without consent did not constitute an "egregious breach of social norms."

However, the court allowed the plaintiffs' state consumer protection and unfair competition claims to proceed. These claims alleged that the defendants' privacy representations were one of the reasons the plaintiffs decided to purchase the devices at a higher price than they otherwise would have paid. Interestingly, the court rejected Apple's argument that all claims should be barred based on certain language in its privacy policy and App Store terms. The court found that the plaintiffs advanced a colorable argument that the terms were ambiguous in relation to Apple's obligations for the collection of personal information. In addition, Apple's disclaimer of liability for third-party actions was not dispositive because Apple made affirmative representations about its efforts to protect privacy. The case is still pending in federal court in California.

(*In re iPhone Application Litig., 844 F.Supp.2d 1040 (N.D. Cal. June 12, 2012).*)

Broader View of Justiciable Harm

The notion of what constitutes justiciable harm in the mobile app arena is evolving to be broader and more permissive than what has been the case for websites. While website operators won early dismissals of website internet tracking claims, recent decisions involving mobile apps have been split on what level of harm is sufficient for certain claims to proceed. This is seen in, for example:

- The Northern District of California's treatment of consumer protection claims in the in re iPhone matter (see *Application of Consumer Protection Laws to Mobile Privacy*).
- Another federal district court's handling of unjust enrichment claims in Goodman v. HTC America Inc..

In *Goodman v. HTC*, end users sued a mobile phone manufacturer and app developer. The complaint alleged that a weather app transformed certain smartphones into surreptitious tracking devices by collecting detailed geolocation information and transmitting it to third parties. The court granted the defendant's motion to dismiss on most of the plaintiffs' consumer protection claims for failure to plead fraud-related claims with sufficient particularity. However, it allowed the plaintiffs' California invasion of privacy and Washington unjust enrichment claims to survive. The court found, among other things, that the plaintiffs stated a plausible claim based upon California's constitutional right to privacy with allegations that the defendants:

- Continuously tracked the plaintiffs' location and movements.
- Sold individualized profiles containing this information.

(*Goodman v. HTC America Inc., 2012 WL 2412070 (W.D. Wash. June 26, 2012).*)

On the unjust enrichment claim, the court found the plaintiffs had adequately alleged that the defendants benefited from smartphone sales that would not have occurred if the plaintiffs had been fully informed of the tracking functionality. Following the court's order, the matter was settled under undisclosed terms.

(*Goodman v. HTC.*)

CHILDREN'S ONLINE PRIVACY AND APPS

In addition to the FTC's general focus on mobile app privacy, in December 2012, the FTC took steps to enhance protection of children's privacy in the online and mobile space, including:

- Implementing substantial revisions to the rules implementing the *Children's Online Privacy Protection Act* (www.practicallaw.com/1-502-2553) (COPPA Rule). COPPA and the COPPA Rule govern practices for collecting and sharing children's information for websites and mobile apps directed to children and for mixed audience sites. The new rule will become effective July 1, 2013. (*78 Fed. Reg. 3,971-4,014 (January 17, 2013) (to be codified at 16 C.F.R. Part 312) and see also COPPA Rule Changes.*)

- Announcing that is has started an aggressive slate of investigations and enforcement actions that will continue in 2013.
- Issuing a report, entitled *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, which disclosed its findings that:
  - mobile apps for kids often lack privacy policies; and
  - even when there are policies, they are often grossly inaccurate.

  Additionally, the report found that kids' apps often link to social media web services without the parental notice and consent the COPPA Rule requires. In many cases, these social media services specifically require their visitors to be 13 or older. For more on this FTC report, see *Legal Update, FTC's Second Kids' Report Reveals Survey Results for Mobile Applications* (www.practicallaw.com/4-523-0485).)

COPPA Rule Changes

The new COPPA Rule is the most significant piece of internet regulation in at least a decade. It has the potential to rewrite the web economy for mobile apps as well as websites that are directed to children.

Broader Scope of Covered Entities

The first major change involves an expansion of the types of entities covered. The new COPPA Rule clarifies that in certain cases it covers third parties that collect information through child-directed sites or services. This includes ad networks and third parties that provide downloadable plug-ins that collect information through child-directed sites and services. These changes significantly increase the number of entities that must now concern themselves with COPPA. (*78 Fed. Reg. 3,971-4,014 (January 17, 2013) (to be codified at 16 C.F.R. Part 312).*)

Expanded Definition of Personal Information

The new COPPA Rule also broadens the category of information it protects by expanding its definition of personal information. Previously, personal information included primarily:

- First and last name.
- Date of birth.
- Social security number.
- Street address.
- Similar kinds of information.

The definition now includes:

- Geolocation information.
- Photos, videos, and audio files that contain a child's image or voice.
- Persistent identifiers that can be used to recognize a user over time and across different websites or online services including, for example, IP addresses and hardware IDs. However, it excludes persistent identifiers that are used purely for the internal operation or maintenance of the site or service.

(*78 Fed. Reg. 3,971-4,014 (January 17, 2013) (to be codified at 16 C.F.R. Part 312).*)

Therefore, the new COPPA Rule applies broadly to passive tracking on mobile apps and websites directed to children. This reflects a dramatic shift by the FTC.

Obtaining Parental Consent

The amendments to the COPPA Rule add several new methods that operators can use to obtain verifiable parental consent including:

- Electronic scans of signed parental consent forms.
- Video-conferencing.
- Use of government-issued identification.
- Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card or other payment system that provides notification of each discrete transaction to the primary account holder, together with an appropriate COPPA disclosure.

Operators also may continue to use the longstanding e-mail-plus mode of consent, where operators that collect children's personal information for internal use only may obtain verifiable parental consent with an e-mail from the parent. Companies participating in an FTC-approved safe-harbor program may also use any consent method approved by such program.

(*78 Fed. Reg. 3,971-4,014 (January 17, 2013) (to be codified at 16 C.F.R. Part 312).*)

Effect of Changes on Using Device and Network Identifiers

In the mobile context, the important practical effect of the expanded definition of personal information is that developers and publishers of covered apps will now be prohibited from sharing device or other persistent identifiers with ad networks, ad exchanges and social networks, in the absence of parental consent. Affected persistent identifiers include, among others:

- Apple's new IFA.
- IP addresses.
- UDIDs.
- Open UDIDs.
- MAC addresses.
- IMEIs.

ACHIEVING COMPLIANCE AND REDUCING RISK

There is no single approach to managing and reducing risk in the mobile space that will be best for every company. Each company should tailor a policy that takes into consideration its own:

- Business needs.
- Available resources.
- Risk exposure.

However, adopting a holistic approach that considers both the surface functionality and hidden technical characteristics of

a mobile app can significantly reduce risk. Awareness of the technical privacy characteristics of an app can make compliance and risk management much easier.

This is particularly critical given the role played by independent researchers. The key players in the mobile arena, including the media, the plaintiffs' bar, the FTC and state regulators, often rely on the highly technical work performed by independent researchers. Therefore, companies must assume that their mobile apps will be reviewed and analyzed by individuals who are sensitive to which technical characteristics:

- May cause privacy problems.
- Are privacy enhancing.

This means that privacy compliance and risk reduction requires that a company learn the detailed technical story of its apps, especially as it relates to privacy. Key practices a company should consider employing to successfully manage mobile app privacy risk include:

- **Privacy by design.** Begin with privacy-by-design in mind. A business should:
  - not collect information it does not need;
  - enable consumer choice and opt-outs of data collection where possible; and
  - provide for secure transmission and storage of personal information and device identifiers.

  (See *FTC Privacy Report*.)
- **Security by design.** Begin with security in mind. For example, viaForensics, a digital forensics and security firm, publishes on its *website* 42 security design principles.
- **Knowing the business rationale.** A company should only collect and share information where there is an articulated business reason for doing so. As a best practice, this should include documenting, internally and in writing:
  - why it is necessary to collect or share certain categories of information; and
  - what privacy protections and safeguards will be employed.
- **Technical control.** A company should maintain technical control over the code supply chain of its mobile apps to ensure it is aware of all ways the apps collect, store, use and share information. This includes requiring developers to disclose:
  - the existence of all third-party code included in the mobile apps' source code;
  - the function of the third-party code; and
  - the third-party network traffic the code may trigger.
- **Legal control.** A company should contractually require all third parties involved in the development and deployment of its apps to adhere to the company's or more restrictive privacy practices. The company should memorialize that requirement in a signed contract.
- **Commissioning a privacy review or audit of network traffic.** Have a privacy review performed of the actual network traffic associated with your mobile app. A best practice is to assume it will be tested by others and any identified vulnerabilities may result in liability or adverse media attention.
- **Commissioning a privacy review or audit of local storage.** Have a privacy review performed of your app's local, app-specific storage.
- **Not collecting hardware IDs.** If possible, do not collect persistent identifiers.
- **Protecting location data, photos, and audio and video files as personal information.** Minimize, if possible, the collection of GPS or other geolocation information and information associated with photos, audio files and videos.
- **Using opt-outs.** Enable end users to opt out of information collection and sharing, if possible.
- **Complying with industry-specific laws and best practices.** Consider whether the app may be subject to industry-specific regulation and seek industry-specific guidance, for example, in the areas of:
  - healthcare information (consider the *Health Insurance Portability and Accountability Act* (www.practicallaw.com/1-501-6222) (HIPAA));
  - medical devices (consider rules and guidance by the *Food and Drug Administration* (www.practicallaw.com/3-501-7065) (FDA));
  - financial services (consider the *Gramm-Leach-Bliley Act* (www.practicallaw.com/7-501-3428));
  - data broker regulation (consider the *Fair Credit Reporting Act* (www.practicallaw.com/4-502-8855) (FCRA)); or
  - child-directed content (COPPA; see *COPPA Rule Changes*).
- **Developing a short form and long form privacy disclosure.** The short form should:
  - provide a succinct overview of the information collection and sharing practices of the mobile app;
  - disclose collection and sharing of any personal information, geolocation data, hardware IDs, photos, address book data and audio files; and
  - link to a longer policy that provides additional detail for the end user.

  For additional materials on these points, see *Privacy Multistakeholder Process: Mobile Application Transparency* on the US National Telecommunications and Information Administration's website.
- *Adhering to industry self-regulatory guidelines.* For example, the Mobile Marketing Association published the Mobile Application Privacy Policy Framework, which sets out guidelines to address core privacy issues and data processes of mobile apps. The framework includes model policy language (see *Legal Update, Mobile Marketing Association Releases Privacy Policy Guideline for Mobile Apps* (www.practicallaw.com/8-517-6924)).

The measures set out in this Note are not exhaustive. Companies may also need to consider other factors based on their specific business concerns. The issues examined above should be the starting point for discussion and internal dialogue for generating better compliance strategies.

WEBSITE INFORMATION COLLECTION

In the website context, end users access almost all online content using internet browser software. Typically, this access is through desktop and laptop computers, though mobile browsers also provide access to both PC-oriented and mobile-optimized websites. Companies seeking to interact with consumers or the general public through this model do so by creating an engaging website that provides, for example, games or e-commerce functionality. Key features of the browser-based internet are that:

- Much of the software, content, and databases that enable this wide assortment of services are located remotely on website servers.
- Most information collection, sharing, and storage is mediated by the browser. Therefore, end users typically can manage information collection and storage centrally through browser tools and settings.

However, note that some website information collection and storage occurs locally outside the browser, including by local shared objects. The most common example of these is Flash cookies. Other less common mechanisms include device and browser fingerprinting, which catalog unique characteristics about a particular computer including, for example, the operating system and browser.

Browser-based Privacy Framework

Websites collect and store end user information by using, among other things:

- Brower cookies.
- Other browser-stored information, including the browser cache and e-tags.
- HTML5 local storage.

For example, to enable a third party to display advertising on its web pages, website operators include small pieces of JavaScript code or script "tags" on their web pages. These scripts or tags cause the end user's browser to establish network connections to the third party's servers, even though:

- The end user has not left the website.
- This network connection is not apparent to the lay end user.

Through these network connections, these third parties can:

- Place, read and modify their own cookies.
- Gather detailed web-browsing information about end users as the users navigate the many websites that embed the third parties tags.

Browser Cookies

When an end user visits a website, the site may serve cookies, which are then stored locally on the user's computer. When the user visits that website, the browser transmits the cookies back to that website's servers. Cookies can store many types of data, including:

- Information the end user provides (for example names, street addresses and zip codes).
- Information the website provides that has semantic meaning (for example, user account numbers, shopping cart information, IP addresses, and website pages viewed).
- Unique numbers and character strings generated by the website that carry no independent meaning, but uniquely identify an end user's computer to the website's servers.

As an end user navigates a website, the constant transmission of cookies from the end user's computer can provide rich information to the website operator. Cookies placed on an end user's computer may be from either:

- The website the end user is visiting (first-party cookies).
- Third parties the website operator engages to provide, for example:
  - targeted advertisements;
  - social network options; or
  - website analytics.

Browser Privacy Controls

Responding to privacy concerns associated with websites and third parties remembering browsing history or building end-user profiles, the major browser software providers now provide privacy controls including:

- Detailed menus and options for deleting, managing, and blocking browser cookies.
- Browser add-ons and plug-ins exist that also allow for the detection and deletion of Flash cookies and other types of locally stored information.

Industry consortia have also established self-regulatory regimes for using cookie technologies to prevent certain types of tracking and ad targeting. For more on industry self-regulation of behavioral advertising, see *Practice Note, Online Advertising and Marketing: Online Behavioral Advertising* (www.practicallaw.com/4-500-4232) and *Direct Marketing Association* (www.practicallaw.com/4-500-4232).)

Therefore, while the traditional desktop and laptop environment is complex, it also provides end users with many well-developed and evolving solutions to reduce tracking. Note that the privacy issues discussed in this section concern day-to-day tracking in the business-to-business and consumer context. This discussion does not suggest that browser tools are sufficient to frustrate tracking efforts by, for example, governmental authorities, hackers, or law enforcement. The Tor Project provides a discussion of various tools necessary to achieve stronger anonymity on its *website*.

For the links to the documents referenced in this note, please visit our online version at http://us.practicallaw.com/8-523-6918.

For more information on mobile app privacy, search for the following resources on our website.

Practice Notes:

- *Online Advertising and Marketing (http://us.practicallaw.com/4-500-4232)*

