# Transparency

## A Brief Future of Privacy Forum Survey of Mobile Application Best Practices

This document has been assembled to provide an overview of some efforts to date to develop guidelines that contribute to transparency. There is a good deal of work to be done; nonetheless, this document seeks to be a helpful addition to the discussion by highlighting and bringing to the table some of the work previously done by some participants. We recognize that none of these documents received the full scrutiny and input from the wide range of stakeholders in the NTIA process and thus they should certainly not be considered a first draft or a consensus document. And we recognize the importance of considering the best path to including the key deliverables which go beyond guidelines, as raised by some stakeholders, including legislation, accountability, and other issues. But we think the below may be useful for beginning a portion of the work to be done, which certainly includes guidelines for app developers and others in the ecosystem.

**SOURCE DOCUMENTS**

This document draws on transparency recommendations that appear in the following documents. In addition to below, links to the documents can be found at this page of the FPF Application Privacy site. Since app platforms usually require developers to provide certain privacy information in their developer agreements, we highlight some of those clauses at the end of this document.

1. FPF and CDT Best Practices for Mobile Applications Developers
2. Information and Privacy Commisisoner of Ontario Roadmap for Privacy by Design in Mobile Communications
3. GSMA Model Application Privacy Program
4. MMA Mobile Application Privacy Policy Framework
5. EFF's Mobile Bill of Rights
6. Microsoft's Privacy Guidelines for Developing Software Products and Services
7. CTIA's Best Practices and Guidelines for Location Based Services
8. Lookout Mobile Security's Mobile App Advertising Guidelines
9. FTC Staff Report: Mobile Apps for Kids
10. DAA Self-Regulatory Principles for Online Behavioral Advertising
11. The State of California Office of the Attorney General Joint Statement of Principles
12. Happtique App Certification Program Draft App Certification Standards

**PRIVACY POLICY RECOMMENDATIONS**

A significant step toward respecting user privacy is creating a privacy policy that explains what data is collected, how data is used, and with whom data is shared. Although there should be other places within an app where specific disclosures are provided to users, the privacy policy should contain a comprehensive overview of the data collection and use practices. The more information that you collect and use, the more detailed your privacy policy should be.

Failure to disclose material information or a misstatement regarding data use practices disclosed in a privacy policy (or elsewhere), could serve as grounds for government investigations, enforcement actions, and private lawsuits.

We recognize that a privacy policy is only one element of this discussion, but since it is a key leverage point for enforcement action under current law, we begin our discussion with this requirement.

**1. Transparent Disclosures**

At a high level, most of the best practice documents reviewed reference the importance of transparency. Others incorporate transparency by reference. Most have requirements that fall under transparency.

Example Recommendations

- EFF: *Users need to know what data an app is accessing, how long the data is kept, and with whom it will be shared. Users should be able to access human--readable privacy and security policies, both before and after installatio*n.
- FPF and CDT: *Be clear and specific in disclosures. Uses of user data listed in a privacy policy should be specific and include what personal information an app accesses, collects, uses, and shares and the purpose for such collection. Uses of data that are not explained in a privacy policy should be prohibited*.

THIRD PARTIES

Some groups called for notice within a comprehensive privacy policy when third parties were involved.

Example Recommendations

- FPF and CDT: *To the extent that it is practical, privacy policies should disclose the names and websites of the third parties (if any) with whom user data is shared. At a minimum,*

*a comprehensive privacy policy should identify the types of companies with whom user data is shared.*

- Lookout: *App Publishers should display information related to data collection by third parties or unexpected non-app publisher sources in a manner that makes this distinction clear and obvious.*

LINKING TO DEVICES OR RECORDS

Some groups called for notice within a comprehensive privacy policy when mobile user data would be linked to a particular record or device.

Example Recommendations

- FPF and CDT: *Inform users if their data can be linked back to a particular record or device, even if user data is not tied to a real name (traditionally called "personally identifiable information," or "PII"). People have a privacy interest in "pseudonymous" or "anonymous" data if that data is used to customize or alter the user's experience, or if it could reasonably be linked back to the individual through re-identification or through a government subpoena, or other legal means.*
- Lookout: *The collection, usage, and storage of data that can be used to uniquely identify a user or their device must be performed in ways that are consistent with the context in which users provide that data, and accompanied by methods of user notice that reflect the relative privacy implications of such data.*

**2. Accessibility**

Some of the best practices addressed user access to privacy policies before they download and install the app and the location that users can find the privacy policy.

ACCESS PRIOR TO DOWNLOAD

There is general agreement that it is a best practice to provide privacy information and/or a hyperlink to a privacy policy prior to download.

Example Recommendations

- EFF: *Users should be able to access human-readable privacy and security policies, both before and after installation.*
- FPF and CDT: *Give your users easy access to your privacy policy before they download and install the app. This means including a link to your privacy policy from your app store listing, or include a link in the sign-up page that appears before users have full access to the app. If the app store framework limits your ability to do this, make sure to include your privacy policy in the app itself.*
- Lookout: *In cases where Personal Information is collected (which can include name, phone number, email address, fine-grained location information, or more), simply providing detailed privacy policies may not be sufficient and requires gathering informed*

*consent from users through the use of conspicuous, clear notification techniques prior to enabling data collection. This guideline has clear implications for App Publishers, but is especially important for Ad Providers, with whom mobile users rarely directly interact knowingly.*

POLICY LOCATION PROMINENCE

Placing the app privacy policy in a prominent location is suggested my several of the groups.

Example Recommendations

- State of California Office of the Attorney General: *Where applicable law so requires, an application ("app") that collects personal data from a user must conspicuously post a privacy policy or other statement describing the app's privacy practices that provides clear and complete information regarding how personal data is collected, used and shared.*
- FPF and CDT: *Don't make users search for it; place your full privacy policy in a prominent location within the app under a "Privacy Policy" menu heading or under the Settings menu. If it's not possible to do this, provide a hyperlink to your privacy policy in similar location. The link should take users directly to the policy with a minimal amount of click-through. Upon retrieval, the policy should adjust to fit the size of the mobile screen*.
- GSMA: *Responsible persons shall be open and honest with users and will ensure users are provided with clear, prominent and timely information regarding their identity and data privacy practices.*
- Microsoft: *A "Prominent Notice" is one that is designed to catch the customer's attention. An example of a Prominent Notice is the privacy options page displayed the first time a customer runs Microsoft Windows Media® Player 10. This page invites customers to inspect the current privacy settings, learn more about their options, and make choices.*

**3. Changes to Data Use Practices**

Some of the best practices specify that when new data practices are being planned that new privacy policies must be created and made available to users prior to implementing the changes. The amount of lead-time that is necessary is not commonly specified.

Example Recommendations

- Microsoft: *The privacy implications of software, Web sites, and Web Services may change over time. When customers have given consent for the use of their data, they have consented to the specific use and business purpose disclosed to them. Additional consent must be received in order to use the customer's data for a different purpose. When there is a material change to the privacy implications of an application, Web site, or Web Service, additional notice should be given to the customer.*

- FPF and CDT: *If you change your data practices, give your users advance notice. For example, posting an updated privacy policy 30 days in advance will give your users time to digest the changes and notify you of any questions or concerns.*

**SHORT-FORM NOTICE**

Some groups called for that short form or layered notice, where appropriate, to increase transparency and allow uses to easily browse key data practices. It was often suggested that the full policy by linked to from the short-form notice.

Example Recommendations

- Microsoft: *A "Layered Notice" can make it easier for the customer to understand a complex privacy statement. A layered notice typically includes a single-page summary of the privacy statement (that can be read without scrolling) divided into specific sections (e.g., "Personal Information," "Uses of Information," and "Your Choices"). The summary page includes links to more detail (i.e. specific sections within the full privacy statement). Layered Notices are a recommended practice for Web sites and products with complex, lengthy privacy statements.*
- FPF and CDT: *Consider providing a short form notice – a notice with a limited number of characters that highlights the key data practices disclosed in the full privacy policy – in your app. Seek to provide users with the information needed in the context, at the most relevant time.*

**ENHANCED NOTICE**

Most of the best practice documents reviewed referenced enhanced notice for activities that use sensitive personal information and/or using data in an unexpected way. A privacy policy is not the only place to provide information about data collection and use.

UNEXPECTED USES/ACCESSING USER INFORMATION

Many of the guidelines suggest that apps that use data in an unexpected way should make an extra effort to ensure users understand this and agree to the use of the data.

There was no set definition of "unexpected uses" because the determination depends heavily on context.

The FPF and CDT guidance provided the following list:

- Sharing data with third party advertisers for behavioral advertising purposes
- Sharing data with third parties to allow other transactional data to be appended and used across sites
- Accessing or sharing precise geo-location information
- Accessing contacts

- Accessing other sensors or features on the phone (like a camera or microphone)
- Accessing photos and videos
- Accessing dialer or text messages

The Lookout guidance further called for enhanced notice by advertisers when new Ad Delivery methods like push notifications are employed.

**1. Sharing Data with Third Parties**

Some groups called for additional notice to highlight when data use practices involved the transfer of users' data. Third parties include apps that use third party analytics or by ads.

Example Recommendations

- GSMA: *Users shall be provided with information about persons collecting personal information about them, the purposes of an application or service, and about the access, collection, sharing and further use of a users' personal information, including to whom their personal information may be disclosed, enabling users to make informed decisions about whether to use a mobile application or service.*
- FPF and CDT: *When using third-party code or software development kits (SDKs)—such as those from advertising networks or analytics— make sure you understand what the code is doing and the practices of those third parties and describe it clearly to your users. If you are accepting ads provided by a third-party ad network, it is possible that user data is being used to tailor ads on other apps or that you are passing along unique, fixed device identifiers to that ad network. You should only work with third parties that either do not engage in such targeting or give users choice around such targeting. In either case, your privacy policy should clearly explain that you are sharing behavioral and device identifier information with third parties (when applicable). Identify those third parties and link to information about how to opt-out of such tracking or targeting.*

**2. Location**

Location data is often flagged for receiving special treatment under the reviewed best practices.

Example Recommendations

- CTIA: *Providers must ensure that potential users are informed about how their location information will be used, disclosed and protected so that they can make informed decisions whether or not to use the LBS, giving the user ultimate control over their location information.… Providers must periodically remind users when their location information may be shared with others and of the users' location privacy options, if any.*
- Information and Privacy Commissioner of Ontario: [...] *Notifications are a useful tool for those data elements that can be controlled by the user. For instance, an icon, light or other 'at-a-glance' feedback mechanism could be displayed when the geolocation capability of the device is active, or the data it is generating is accessible to installed applications.*

- FPF and CDT: *You should only collect and transmit such information when you have your users' clear, opt-in permission. While most platforms do require express permission for an app to access location information, if you are using that data in unexpected ways or are transmitting that information to third-parties, make sure you get your own permission from the user before doing so. In your app's privacy policy, specify how you collect, use and share location data. You should also provide disclosure for: (1) the level of location data collection such as precise or fine, zip level, zip+4, or coarse; (2) whether the data is being used with a unique mobile identifier; and (3) the period of time that the user's location data is linked with the user's identifier.*

**3. Camera**

Geo-tagging photos was raised by a small subset of the best practices reviewed.

Example Recommendations

- FPF and CDT: *Provide notice about geo-tagging if your app takes photos and/or videos. Geo-tags and related metadata may reveal the location coordinates where the photo or video was taken. Since users are not always aware this is happening, provide notice explaining that geo-tagging may occur.*

**4. Automatic Sharing**

Several of the best practices reviewed suggested enhanced notice if an app engages in frictionless sharing.

Example Recommendations

- MMA: *Mobile application developers should be aware of which mobile advertising networks and other third parties they are working with in order to determine if that ad network or other third party is offering an opt-out. At a minimum, application developers should take into account whether the app is advertising supported and whether data is obtained by an ad network or other third party for the purpose of ad targeting*.
- FPF and CDT: *If your app engages in frictionless sharing, make sure that users know when automatic sharing is enabled by providing clear notice and follow platform auto-sharing delay rules.*

**5. Enhanced Notice by Advertisers**

A few of the best practices reviewed suggested enhanced notice if an app engages in some forms of advertising.

Example Recommendations

- Lookout: *Provide context and control when experimenting with new Ad Delivery Behavior. Mobile Ad Providers have recently started to explore new methods of ad delivery, including delivering ads in the system notification bar (also known as "push" notification ads), placing new icons or shortcuts on the mobile desktop, and modifying*

*browser settings such as bookmarks or the default homepage. When an ad is delivered outside the context of an individual application, mobile users have a right to know where the ad came from and how they can take action to control such behavior. More specifically:*

- *Ad Providers experimenting with push notification ads must provide clear attribution to the source host application responsible.*
- *Ad Providers that modify browser settings or add an icon to the mobile desktop must provide clear, conspicuous notice to users and gain explicit consent prior to doing so.*

- DAA: *The "enhanced notice" approach required by the Transparency Principle will offer consumers the ability to exercise choice regarding the collection and use of data for online behavioral advertising through one of several avenues. Links to consumer notices will be clear, prominent, and conveniently located. This enhanced notice will be provided at the Web sites from which data is collected. Such enhanced notice will be provided at the time of such collection and use, through common wording and a link/icon that consumers will come to recognize. The opportunity for Web site users to exercise choices about whether Web viewing data can be collected and used for online behavioral advertising will never be more than a few clicks away from such standardized wording and link/icon.*[1]

SENSITIVE USES

There is no set definition for "sensitive uses" but the FPF and CDT guidance suggests that it includes data related to:

- Health
- Finances
- Race,
- Religion,
- Political affiliation,
- Political party membership, and
- Sexuality
- Children

**1. Health**

A few of the best practices reviewed suggested enhanced notice if an app uses health data.

Example Recommendations

[1] These are the DAA Self-Regulatory Principles for Online Behavioral Advertising, which apply to websites. DAA mobile application rules are not yet publicly available. We reference them here to point out the concept of enhanced notice when certain types of advertising are involved, and await release of DAA mobile guidelines for an industry view of enhanced mobile notice.

- FPF and CDT: *If your app collects or transmits data associated with any of these categories, you should make an extra effort to ensure your users understand this and expressly agree to its use. Sensitive user data warrants stronger protections and often carries specific legal requirements.*
- Happtique: *The user has the ability to access or request any of his/her Protected Health Information (PHI) collected, stored and/or transmitted by the app, and has the ability to learn the identity of any person or entity who had or has been granted access to his/her PHI.*

**2. Children**

Several of the best practices reviewed suggested enhanced notice if an app is directed at an audience of children.

Example Recommendations

- FTC: *Although the two major U.S. mobile app stores provide some information and controls governing apps, all members of the mobile app ecosystem – the app stores, the developers, and the third parties providing services within the apps – must do more to ensure that parents have access to clear, concise and timely information about the apps they download for their children. Parents should be able to learn, before downloading an app for their children, what data will be collected, how the data will be used, and who will obtain access to the data. Armed with such information, parents can make knowledgeable decisions about the apps they choose for their children, and embrace these technologies with more confidence.*
- FPF and CDT: *Avoid sharing kids' or teens' information with third parties and provide clear, age-appropriate notice about any data you do collect or share. In a recent Staff Report, the FTC expressed disappointment in the high number of children apps' that fail to disclose their data collection and use practices prior to download. Ensure that parents are able to make an informed decision before installing your app.*

**APPENDIX: APP STORE PLATFORM REQUIREMENTS**

**APPLE**: Developers must provide clear and complete information to users regarding collection, use and disclosure of user or device data. (Section 3.3.10 of the iOS Developer Program License Agreement) Apps should have all included URLs fully functional when you submit it for review, such as support and privacy policy URLs. (Section 3.12 of the App Store Review Guidelines) Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used. (Section 17.1 of the App Store Review Guidelines)

**ANDROID**: If users provide you with, or your app accesses or uses user names, passwords, or other log-in or personal information, you must make users aware that this information will be

available to your app, and you must provide legally adequate privacy notice and protection for those users. (Section 4.3 of the Android Market Developer Distribution Agreement) It is important to respect user privacy if certain parameters, such as demographics or location, are passed to ad networks for targeting purposes. Let your users know and give them a chance to opt out of these features. (Android Training for App Developers - Monetizing Your App: Advertising without Compromising User Experience)

**FACEBOOK**: You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application. (Section II(3) of Facebook Platform Policies)

**INTEL**: If your application collects any personal information, the user must be notified about what is being collected, why it is being collected (purpose) and whether the information will be shared with anyone else. (Section 1.1 of Intel's AppUp(SM) Developer Program Privacy Requirements and Recommendations)

**MICROSOFT**: If your app enables access to and the use of any Internet-based services, or otherwise collects or transmits any user's personal information, you must maintain a privacy policy. Your privacy policy must (i) comply with applicable laws and regulations, (ii) inform users of the information collected by your app and how that information is used, stored, secured and disclosed, and (iii) describe the controls that users have over the use and sharing of their information, and how they may access their information. If your app uses the geolocation, texting/SMS, webcam or microphone capabilities, you must also provide access to your privacy policy in the app's settings as displayed in the Windows settings charm. (Section 3(f) of the App Developer Agreement)