BEST PRACTICES FOR MOBILE APPLICATIONS DEVELOPERS

SUMMARY

"Mobile applications" — the software programs written to execute on one or more mobile device operating systems (such as Android, Blackberry OS, iOS, Symbian or Windows Phone OS) – can collect and transfer end users' personal information from their mobile devices. Such transfer of personal information raises privacy issues. And privacy in mobile applications can be a challenge. Mobile platforms may have terms of use related to privacy but it is not always clear what those terms mean. Most developers are not experts in privacy law and policy and do not have the resources to hire lawyers or privacy consultants. The small screens of mobile devices limit the amount of information that can be easily communicated to users. Moreover, it may be difficult to understand how the third-party services incorporated into apps, such as analytics packages and those from advertising networks, use and access end users' information.

Although this document is aimed at app developers, we recognize that the ability to comply with leading practices described here may depend on other parties such as platforms, advertisers, ad networks and others. In some cases, providing the right notice and choice to the user may be best implemented by some of those other parties. Nonetheless, it is important to understand that as an app developer, you, rather than the platform or third-party services, have the most significant legal and ethical obligations to your users. Many countries place obligations on companies that collect, use, or transmit personal data. In the United States, the Federal Trade Commission has recently brought a number of enforcement actions against application developers accused of misusing user data. Nearly all app marketplaces require that you provide a written privacy notice if your app transmits data from the device.

One important thing to keep in mind is that many, if not most, privacy issues for application developers come from inserting third party code or software development kits(SDKs)—such as those from advertising networks or analytics providers—into your app. If you plug someone else's code into your application and then release it to a user without understanding how it collects, uses, or transmits your users' information, you are on the hook both legally and to users, with regard to the third parties you work with, and the analytics/practices they engage in. Make sure you understand what your third party providers are doing with user data, and make sure your users are informed and have control over how their information is used.

The following recommendations are based on the Fair Information Practice Principles— a set of generally accepted principles for how organizations should treat individuals' personal information. These principles include:

- Be completely transparent about how you are using or transmitting user data
- Don't access more data than you need, and get rid of old data
- Give your users control over uses of data that users might not expect
- Use reasonable and up-to-date security protocols to safeguard data

- As the app developer, you need to be responsible for thinking about privacy, and taking privacy into consideration during the various stages of your app life cycle

This document outlines best practices to guide you in building privacy into your application.

Transparency and Purpose Specification

- ***Have a Privacy Policy.***[1]

  The first step in respecting your users' privacy is to create a privacy policy that explains what you do with their data, and with whom you share it. This is an important process, even if you do not believe that you are collecting or using data that would trigger privacy concerns. The more information that you collect and use, the more detailed your privacy policy should be. Note that almost all applications collect information in some manner and for different purposes. If you are not actively collecting personal data, you are probably passively collecting personal data for authentication or similar purposes. If your app uses third party analytics or is ad supported, you are likely collecting or disclosing user information.

  Do not just cut and paste a privacy policy from another app or website. Start by understanding *your* app in your own terms, and then do your best to communicate the same to your users. If you are using third-party code in your application, make sure you understand what those third parties are doing, and describe it clearly to your users. If you misstate what you are doing in your privacy policy (or elsewhere), you may bear legal responsibility for deceiving your users.

  Companies like PrivacyChoice and TRUSTe provide excellent (and, to some extent, free) tools to help you create your own policies and short-form notices to your users. The Mobile Marketing Association has also put out a model privacy notice that can help guide the creation of your own policy. And the Future of Privacy Forum provides privacy resources for app developers at ApplicationPrivacy.org.

  Provide a link to your privacy policy in each app store listing and on your own site so that users can review it before downloading your app. Platforms and application stores should ensure that apps are able to provide a privacy link in advance. If your app has a settings page, place a privacy policy link there as well, and make sure that it leads to a page that can easily be read on a mobile device.

[1] When developers sign up with a platform, they agree to the platform's terms of services. However, that is not a privacy policy that covers your relationship with your users.

EXAMPLES:

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)

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)

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 shares a user's personal information (including, but not limited to Contacts, Photos, Phone number, SMS, Browsing history or unique device or user IDs combined with user information) with third parties, the application must implement a method to obtain "opt-in" consent. (Section 2.8 of the Certification Requirements)

- ***Make extra effort to disclose and communicate unexpected uses of user data.***

  A privacy policy is an important resource to help users, advocates and regulators understand your practices, but it is not the only place you should provide information about data collection and use.

  If your app makes use of data in a way that users might not expect, you should make clear, conspicuous and timely disclosures of that fact.

  Depending on the type of app, some unanticipated uses might include the following:

  - Sharing data with an ad network for behavioral advertising use
  - Working with third parties to allow other transactional data to be appended and used across sites
  - Accessing or sharing precise geo-location sensitive information
  - Accessing contacts

- Accessing other sensors or features on the phone(like a camera or microphone)
- Resetting a user’s browser homepage
- Installing toolbars
- Changing default search

In many cases, it may be obvious to the user why you are collecting data. For example, if your app provides local restaurant reviews and asks a user for permission to access their current location, that purpose is obvious. However, if your app also transmits location information to third-party advertisers, that may not be obvious to users. In that case, your notice might say, "We need your location information to select restaurants near to you, and also so that our advertising partners can show more relevant advertising based on your location."

Platforms and applications stores should consider steps they can take that would allow apps more opportunity to explain the reasons why certain types of data are required in the app download or authorization process.

Even if user data is not tied to a real name (traditionally called “personally identifiable information,” or “PII”), you should still inform users if the data is linkable back to a particular record or device. 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 reidentification or through a government subpoena (or other legal means).

- ***Share new data use policies before implementing them to give your users notice and time to understand them.***

  Whenever you update your app, review your privacy policy to confirm that it accurately describes your current data practices. 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. If your updated policy includes a new, unexpected usage of any data (including pseudonymous data), especially unexpected transfers of information to third parties, you should be especially clear and conspicuous in your notice. When you post a new policy, tell your users upfront what has changed, so they do not have to parse through the old and new policy to see what is different.

  A simple way to notify users of privacy policy changes is to include the date of the most recent update in the anchor text of your policy link, such as "Our privacy policy (updated 10-28-11)."

Use Policies and Limitations

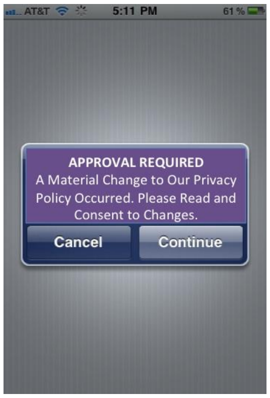
- ***Be clear and specific in your disclosures.***

  When you issue your privacy policy, be specific when you list uses of user data. Do not be ambiguous or try and reserve all rights to the data. To the extent that it is practical, also disclose the exact third parties (if any) with whom you share your users' data. If nothing else, you should clearly identify the *types* of companies with which you share user data. If you cannot clearly articulate to users a reason why you are collecting certain data, do not collect it.

- ***Stay within the boundaries of your disclosures; don't use or collect data if you haven't explained the practice to the user.***

  If you have not explained a particular use of your users' data in your privacy policy (or elsewhere), do not use the data in that way. Undisclosed data practices can get you into trouble with the FTC or other regulators. Obviously, you may not be able to envision every possible use of user data when you write a policy, but try to keep your policies up-to-date as your data usage practices change.

- ***If you make material changes to your data policies and practices, get new permission from your users before using old data.***



APPROVAL REQUIRED

A Material Change to Our Privacy Policy Occurred. Please Read and Consent to Changes.

  If you make a material change or update to your data use policies, you should obtain affirmative, opt-in consent from your users before using previously collected data in new ways. In the U.S., the FTC and State Attorneys General have brought enforcement actions against companies that tried to retroactively change privacy policies to allow for new data uses. (And do not rely on language in a privacy policy that reserves the right to change the policy at any time — courts have found those to be unfair and invalid.)

- ***Don't access or collect user data unless your app requires it.***

  Don't take what you don't need. If you gather or transmit data that your app does not need for a legitimate purpose, you put both yourself and your users at risk. Advertising may well be a legitimate purpose—so long as the collection and transfer of targeting data is transparent, and users are given options about usage of their information for that purpose (see "Individual Choice," below).However, platform and app stores may have their own rules about the collection and use of user information for certain purposes, including advertising. Violating a platform's terms of service could get you in trouble with the platform or app store, or with regulators who assert

Apple obtains information about the device's precise location (the latitude/longitude coordinates) when an ad request is made. However, Apple immediately converts the precise location data to the five-digit zip code, and then discards the coordinates. Apple does not record or store the precise location information, only the zip code. (Apple letter to Rep. Markey on location, May 2011 .)

that a platform or app stores’ rules create reasonable expectations on the part of the user about how their information will be treated. Delete data that does not need to be retained for a clear business purpose.

- ***Delete old data*.**

Get rid of user data that you don’t need anymore. Don’t just keep user data around indefinitely on the off-chance that it may be valuable some day. This applies whether you store user data on the device, or your own servers, or in a cloud platform. Remember to clear associated metadata or cross-references to deleted data. These practices respect your users’ privacy interests and helps protect you and users in the event of a data breach (if your security is breached, you may be legally responsible for failing to exercise reasonable security procedures, and for informing users that their data has been compromised).In lieu of deletion, deidentification of the data may be sufficient if there is no reasonable chance the data could be linked back to an individual or device. Consider the retention periods of your vendors as well when assessing any third-party service to which you will be sending user data.

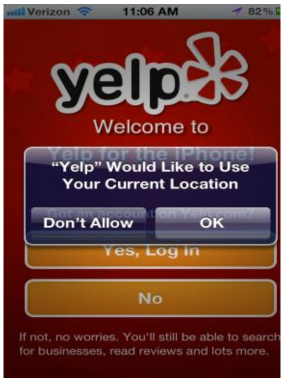
Intel’s developer program states that developers should collect and/or process only the personal information required for a specific purpose and not retain personal information longer than necessary to satisfy the purpose for which it was collected. (Section 3.4 of Intel’s AppUp(SM) developer program Privacy Requirements and Recommendations.)

You should also delete user data promptly following the deletion of an account. Users should rightly expect that once they close their account, all data be deleted from your server.

Individual Choice

- ***Provide stronger protections and enhanced control over sensitive information.***

Sensitive information about your users warrants stronger protections. The definition of “sensitive” may vary from jurisdiction to jurisdiction, but often includes data related to health, finances, race, religion, political affiliation or party membership, and sexuality. If your app collects or transmits data associated with any of these categories, you should make an extra effort to ensure your user understands this and expressly agrees to its use. Simply describing these uses in a privacy policy or terms of use is not sufficient.



“Yelp” Would Like to Use Your Current Location

If not, no worries. You’ll still be able to search for businesses, read reviews and lots more.

Precise geo-location information is increasingly considered sensitive information as well, and 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 transmitting that

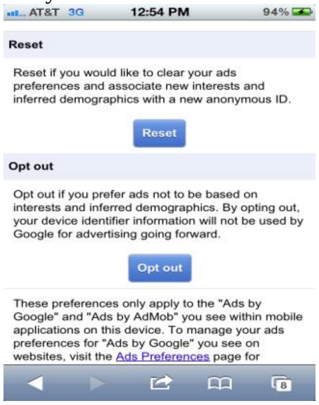
It is important to respect user privacy if certain parameters, such as demographics or location, are passed to ad networks for targeting purposes. Let your users know and give them a chance to opt out of these features. (Android Training for app developers - Monetizing Your App: Advertising without Compromising User Experience.)

information to third-parties, make sure you get your own permission from the user before doing so.

- ***Give users choice around the unexpected collection, storage, or transfer of personal information.***

You should give users meaningful control over their information. If you are collecting or using data outside the scope of what users would reasonably expect, you should at the very least make sure your users can opt-out of such uses of their data. When a user opts-out, you should stop sending personal data to third-party advertising partners (or stop letting third parties access user data from the device or elsewhere) or make sure they have procedures in place to not track users across applications. If your advertising partners offer users the ability to persistently opt-out of the tracking and usage of their data, you can rely on these opt-outs so long as you conspicuously describe and link to those opt-outs in your own policies and disclosures (at least in the United States).

Google To serve ads in applications and other clients where cookie technology is not available, Google hashes users' device ID. Users may choose to reset or opt out of anonymous IDs at any time. If users choose to opt out, ads delivered to your application or other client by Google's ad-serving technology will not be served based on an anonymous ID.



Reset

Reset if you would like to clear your ads preferences and associate new interests and inferred demographics with a new anonymous ID.

Opt out

Opt out if you prefer ads not to be based on interests and inferred demographics. By opting out, your device identifier information will not be used by Google for advertising going forward.

These preferences only apply to the "Ads by Google" and "Ads by AdMob" you see within mobile applications on this device. To manage your ads preferences for "Ads by Google" you see on websites, visit the Ads Preferences page for

If you are accepting ads provided by a third-party ad network, it is quite 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. 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. You should also consider whether you can provide your own functionality to allow users to prohibit transfer to a third party of a unique tracking identifier.

For example, the Digital Advertising Alliance (DAA) principles are one method of providing notice and choice of advertising options.We recognize that the current tracking and user control options available to apps are limited by platform technologies and policies. Cookies are unavailable, as are cookie controls or other tracking control options. Platforms should consider providing users with privacy controls that can be used to block or manage the tracking mechanisms used by third parties. For example, iOS5 provides users the opportunity to opt-out of sharing location with iAds and Android provides users with the opportunity to decline behavioral advertising with Google's AdMob division. Platforms should similarly provide options or APIs that would enable other third parties with similar options to provide users with a choice to opt-out of being tracked or profiled.

You do not, however, have to offer choice around all uses or transfers of data. If the collection and use of the data is obvious and related to the product you offer, it can be assumed that the user has consented to these uses (you should still make sure you describe these uses in your privacy policy). The Federal Trade Commission has recently stated that for “commonly accepted” data usages, such as product fulfillment, first-party analytics, security, and accounting and back-office operations, companies should not have to offer users control around such data uses. In some jurisdictions, regulators may require consent for anything other than purposes that are essential for the operation of the app.

In some jurisdictions, notably the European Union, regulators have called for the provision of express consent in certain circumstances, such as when tracking cookies or other unique identifiers are used for behavioral advertising. If you provide your app to European users, you should carefully follow developments in this area.

- ***If you condition use of your app on the collection and use personal information, educate your users about the trade-off.***

If you want to condition distribution of your app on certain data usage — such as sharing personal information with ad networks — that’s fine. If your application is a “take it or leave it” deal, make a clear value proposition to your users so they understand the exchange. Many users may be happy to share their personal information in exchange for your app. However, you need to be clear and up front in your explanation. Also, note that while CDT and FPF think it may be appropriate for apps in a robust marketplace to require consent to “tracking” in exchange for offering users a service, this practice may soon be prohibited in Europe under recently proposed legislation.

- ***If feasible, let your users have access to the data you keep about them or their device.***

If you are keeping records on your users in the normal course of business, you should try to set up a mechanism so that users can readily see what information you are collecting and storing about them. If you are transmitting data to third parties, such as ad networks, you should try to select partners that also offer users reasonable access to the files created about them. Granting access to such data is legally required in many jurisdictions, such as the European Union. It doesn’t matter whether you live in Europe or not — if you collect information from European users, you may well have the legal obligation to make the information you collect and use available to users.

intel You should provide individuals reasonable access to their personal information so the individual can ensure their personal information is accurate, complete and current (Section 3.3 of Intel’s AppUp(SM) developer program Privacy Requirements and Recommendations).

Also, you should strive to ensure that the user personal information you collect, store, and transfer is as accurate, complete, and up-to-date as is needed for the specific use by the app.

Security

- ***Understand the risks associated with your app, and ensure appropriate and reasonable security measures are in place.***

  Understand the security risks associated with your app such as the sensitivity of information you collect and store, and the number of users using the app. All applications that access, use, or transfer individuals' data should be tested rigorously for security purposes. However, all apps should comply with current and reasonable best practices for security.

- ***Encrypt data in transit (e.g., using SSL/TLS) when authenticating users or transferring personal information.***

  Your app should provide appropriate protections for user data in-transit, especially when that data is authentication data, session data, or personal information. New hacking tools have made snooping on unsecure connections quite simple, especially on unsecured Wi-Fi networks. You can avoid many of these problems by using SSL/TLS for all communications with your server, as modern back-end providers should have little problem scaling SSL even to a large number of transactions.

- ***Encrypt data you store about or on behalf of your users, especially sensitive information and passwords.***

  Whenever feasible, you should ensure you are encrypting your users' data, especially authentication information like usernames, email addresses, and passwords. Storing unencrypted data puts both you and your users at risk in the event of a data breach.

- ***Protect user application data.***

  Make sure users can log out of a session using the mobile client, and that password changes on the back-end side invalidate mobile clients' current sessions. If your application accesses, collects, or stores sensitive data or is a fruitful target for phishing attacks, consider using two-factor authentication such as confirmation text messages, or one-time application-specific passwords.

Accountability

- ***Make sure someone is responsible for privacy.***

  You should have at least one person responsible for making sure that privacy protections are integrated into your product. If you are a one-man shop, then this is your job. This means that:

  - You **review your privacy policy** before each app release, to ensure that it remains accurate and complete,

    - You **keep an archive** of your privacy policy, and ensure that change notices are appropriately posted for users,
    - You **confirm your company's rules** for who can access data internally, to ensure that personal information is only available to team members with a need to see it,
    - You **answer all privacy-related emails** and communication, and
    - You **remain on top of new developments** by following the FTC and other industry organizations.

- ***Practice Privacy by Design.***

  Privacy should ultimately become a consideration central to your design process and considered at all stages of app development. Responsible app development goes above and beyond compliance with regulatory requirements and law; strive to make privacy assurance a default mode of operation. Take privacy into consideration during all phases of the life cycle of your application.

- ***Provide users with a way to contact you and respond to questions and concerns.***

  Provide your users with the opportunity to contact you with questions, concerns, or complaints. This can be accomplished through a simple form accessible from within your app, an email address where your users can contact you, or a feedback forum. Consider highlighting common privacy and security topics. Take the time to review and respond to your users' messages; don't merely provide a means for feedback and then fail to follow up. Good communication is good for privacy and your business.

Special Considerations

- ***Make sure you comply with applicable laws and regulations.***

  In the United States, there is a patchwork of federal and state laws protecting certain kinds of information. Most app developers do not work with user data explicitly governed by a federal law. However, federal laws and regulations do extend to user credit reports, electronic communications, education records, bank records, video rental records, health information, children's information and user financial information. If your app handles information in these areas, you should consult with an attorney or privacy expert.

  You should consider the sampling of federal privacy laws and regulatory agencies listed below. If you think you might be covered, conduct further research and/or seek out some legal advice. By providing an application, you are responsible for compliance with all applicable laws.

    - *Fair Credit Reporting Act of 1970 (FCRA)*
      Sets forth responsibilities for "credit reporting agencies," and entities that provide credit report agencies with data, regarding the preparation and dissemination of personal information in user reports for credit, employment, and other important eligibility purposes.

- *Health Insurance Portability and Accountability Act of 1996 (HIPPA)*
  Sets forth national privacy standards for the protection of individually identifiable health information for certain regulated entities.

- *Children's Online Privacy Protection Act of 1998 (COPPA)*
  Sets forth rules governing the online collection of information from children under 13 years of age, including restrictions on marketing to those under 13 years of age (see below for more information).

- *CAN-SPAM Act of 2003*
  Sets forth rules for the sending of commercial e-mail requiring visible and operable unsubscribe mechanisms, accurate subject lines, and other user protections.

- *Video Privacy Protection Act (VPPA)*
  Sets forth rules generally banning the disclosure of personally-identifiable rental or sales records of audiovisual materials (absent written consent).

- *Gramm–Leach–Bliley Act (GLB)*, aka *Financial Services Modernization Act of 1999*
  Sets forth rules for financial institutions requiring disclosure of privacy policies and user opt-outs for the sharing of personal information.

- *Federal Trade Commission "Unfair and Deceptive" Authority*
  The Federal Trade Commission (FTC) has general authority to policy "unfair or deceptive acts affecting commerce." The FTC frequently confronts online services that are unclear or deceptive in their collection and use of personal information.

In Europe, the legal framework consists of national laws and legislation (e.g. Directives) of the European Union — in some countries there will even be different state law on privacy. This is matched by a number of different agencies with different enforcement mechanisms. The main difference from the United States approach is that *all* data is governed by legal requirements, instead of the relatively narrow sector-specific categories described above.

- *Directive 95/46 of the European Parliament and of the Council of 24 of October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of the data*

  Relevant passages include the obligation to have technical and organizational measures to prevent data leakage (Art. 17); information duties (Art. 10-11) and access rights (Art. 12) and rules on international data transfers (Art. 25 ff.)

- *Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*

Relevant passages include security (Art. 4); confidentiality of communication including the consent requirement for placing information on terminal equipment (Art. 5) and use of location data (Art. 9).

- *Information Commissioner's office (ICO), United Kingdom*

While only one of many data protection authorities in Europe, the ICO has comprehensive information about European data protection law. The UK's guidance is especially relevant because of the new power to fine organizations up to $800,000.

- ***Special considerations for children and teenagers.***

If your app is directed at an audience of children 12 and under, it's likely that you will have to comply with the Children's Online Privacy Protection Act (COPPA). COPPA requires you to obtain "verifiable parental consent" before collecting any personal information -- including name, email address, or phone number -- from a child. So if your app is tailored for young kids, be sure not to request that kind of information unless you have a parent's consent first. (There are specific regulatory guidelines that lay out your options for obtaining verifiable parental consent; you should consult with an expert before attempting to collect personal information from children.)

In general, it's a good idea to treat kids' and teens' data very sensitively. The Federal Trade Commission is actively reviewing COPPA's scope and how it applies to app developers, and youth online privacy is a hot-button issue with legislators, regulators, and the press. Any app that seeks out minors will likely face a lot of scrutiny, so keep your data collection to an absolute minimum. You should avoid sharing kids' or teens' information with third parties and should provide clear, age-appropriate notice about any data you do collect or share.

If your app is aimed at kids, you should not share information with ad networks for the purpose of behavioral advertising or any other party (such as mobile analytics companies).

- ***Stay informed of new developments (like "Do Not Track").***

New privacy rules and policies are developing quickly. As a developer, you should stay abreast of these developments.

For example, the FTC recently recommended a "Do Not Track" regime that would make it easy for users to universally opt-out of tracking across websites online. Major Internet browsers have already implemented "Do Not Track" controls, and many are advocating for similar tools on mobile devices. If mobile operating systems begin to deploy "Do Not Track"-type settings, you should consider how to implement those controls and how your third-party partners respect such controls in order to align with your users' reasonable expectations.

Additional Resources

Future of Privacy Forum Application Privacy Site
PrivacyChoice Mobile Resources
TRUSTe Mobile Privacy Solutions
Mobile Marketing Association
IPC Ontario Privacy By Design