Best Practices for Mobile Application Developers

FPF FUTURE OF PRIVACY FORUM

cdt CENTER FOR DEMOCRACY & TECHNOLOGY

App Privacy Guidelines by the Future of Privacy Forum and the Center for Democracy & Technology

Table of Contents

1 Introduction

2 Basic Steps Towards Building Privacy into your App

3 Notice & Transparency

8 Control & Choice

11 Children

12 Data Retention & Security

14 Accountability

15 Applicable Laws & Regulations

17 Stay Informed

17 Resources

Introduction

"Mobile applications" – software programs for mobile device operating systems (such as Android, Blackberry OS, iOS, or Windows Phone OS) – can collect, use, and transfer users' personal information from a mobile device. As the mobile app developer, you are responsible for thinking about privacy at all stages of your app's life cycle.

Mobile apps are at the forefront of current consumer privacy concerns. High profile media attention[1] and a series of class action lawsuits[2] have prompted close scrutiny of app developer data practices from federal and state regulators.[3] As a result, the U.S. the Federal Trade Commission (FTC)[4] is actively enforcing consumer privacy rights against application developers that surreptitiously access or misuse user data.[5]

Although other actors in the mobile ecosystem may also have access to personal information – including OS developers, device manufacturers, app store platforms, service providers, and advertisers – as the app developer, you are often in the best position to provide notice and disclosure due to the end-user.[6] However, limitations inherent in current mobile architecture can sometimes make it difficult for developers to adequately inform users of data collection, use, and sharing practices.

The guidelines set forth in this document are intended to serve as a road map for you, the mobile app developer, to build privacy into your apps, better inform and empower end-users, and foster trust and confidence in the mobile app ecosystem.[7]

Future of Privacy Forum and Center for Democracy & Technology acknowledge Lia Sheena, Kenesa Ahmad, Aaron Brauer-Rieke, and Erica Newland for their invaluable contributions to this report.

[1] For example, the recent Wall Street Journal's "What They Know" investigative series on Internet-tracking technology and consumer privacy has motivated a number of Congressional and administrative inquiries. See http://online.wsj.com/public/page/what-they-know-digital-privacy.html

[2] Class action lawsuits filed against apps are frequently related to claims that personal data on mobile devices is being surreptitiously accessed, transmitted, maintained, and/or used without users' knowledge or permission. Most recently, a federal class action suit was filed against 18 high-profile apps in Texas on March 17, 2012. http://www.scribd.com/doc/85310203/TX-US-District-Court-Class-Action

[3] For example, California has indicated that all app developers that collect personal information from California residents must have a privacy policy in compliance with California's Online Privacy Protection Act. The policy must detail the type of information collected, how the information will be shared, and how consumers may review and make changes to their stored information. Cal. Bus. & Prof. Code §§ 22575-22579.

[4] The FTC is the main consumer privacy protection agency. The FTC derives its enforcement power from Section 5 of the FTC Act which prohibits unfair or deceptive practices under 15 USC § 45(a).

[5] In the FTC's first case involving mobile apps, W3 Innovations agreed to pay $50,000 to settle FTC allegations that it had violated the Children's Online Privacy Protection Act by illegally collecting and disclosing personal information from children younger than 13 without their parents' consent. (August 2011, http://ftc.gov/os/caselist/1023251/index.shtm)

[6] Note that in some instances, the ability to comply with leading practices may depend on some of these other parties. We urge the other key actors in the ecosystem to cooperate with app developers to make the improvements needed to ensure that consumers are provided with the necessary transparency and controls called for in this document.

[7] Many of the guidelines in this document are based on the Fair Information Practice Principles, a set of generally accepted principles that should inform an organization's handling of individuals' personal information. http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Basic Steps Towards Building Privacy into your App

1 Practice Privacy By Design

Be proactive. Ask important questions and embed privacy measures throughout the lifecycle of your product or service.

2 Communicate Openly & Effectively

Have a comprehensive and transparent privacy policy covering all of your data collection, sharing, and use practices. Use clear and simple language.

3 Make Your Privacy Policy Easily Accessible

Don't make users search for your privacy policy – make it prominent and easy to find.

4 Use Enhanced Notice

Don't surprise users – have respect for context. Use enhanced notice in situations where users might not expect certain data to be collected.

5 Provide Users with Choices & Controls

Empower users. Allow them to choose and control the way their data is collected and used.

6 Secure Your Users' Data!

Always use appropriate and up-to-date security measures to protect user data.

7 Ensure Accountability

Make sure someone is in charge! Designate a privacy guru or make sure to explicitly assume the responsibility yourself.

Notice & Transparency

PRIVACY POLICY RECOMMENDATIONS

The first and most significant step toward respecting your users' privacy is creating a privacy policy that explains what data you collect, how you use it, and with whom you share it.[8] Although there may be other places within your app where you provide specific disclosures to your users,[9] your privacy policy should contain a comprehensive overview of your data collection and use practices. Building a privacy policy 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.

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.

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

1. Transparent Disclosures

Be clear and specific in your disclosures. When you issue your privacy policy, be specific when you list uses of user data. Include what personal information your app accesses, collects, uses, and shares and the purpose for such collection. Do not be ambiguous or try and reserve all rights to the data. To the extent that it is practical, also disclose the names and websites of the 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), then don't do it. Undisclosed data practices can get you into trouble with the FTC or other regulators. While you may not be able to envision every possible use of user data when you write a policy, keep your policies up-to-date as your data usage practices change. Inform users when they are updated.

[8] The terms of service or privacy policy developers agree to when signing up to use a certain platform only binds the developer and platform. In other words, those agreements do not cover your relationship with your users.

[9] Other places where an app can provide specific disclosures are before download and installation, in the app store listing, or before accessing data, once the app has already been downloaded.

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.[10]

To help app developers create transparent privacy policies, the Mobile Marketing Association has released a model privacy notice that can help guide the creation of your own policy. The Future of Privacy Forum's site for app developers, ApplicationPrivacy.org, also lists the latest privacy policy tools and resources.

2. Accessibility

Provide a hyperlink to your privacy policy prior to download.[11] 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[12] 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 (see below).[13]

Place your privacy policy in a prominent location. 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.[14] Upon retrieval, the policy should adjust to fit the size of the mobile screen.

3. Changes to Data Use Practices

Prior to updating your app or adopting a new data use practice, review your privacy policy to confirm that it accurately describes your new practices. If your new data use practices are not currently described in your policy, update your privacy policy to include such practices. You should be especially clear and conspicuous in your notice if your updated policy includes new, unexpected uses of any data (including pseudonymous data), especially those related to unexpected transfers of information to third parties. Also, do not use language that reserves the right to change the policy at any time — courts have found this practice to be unfair and invalid.

[10] The Federal Trade Commission recently issued policy recommendations on how to prevent re-identification of data. De-identification is an evolving data protection practice and is discussed further in the Security Measures section in Data Retention & Security on page 13.

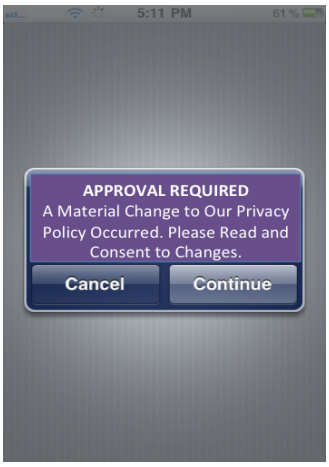
[11] Due to legislative pressures, today, nearly all app platforms must enable developers to provide privacy disclosures to users. In February 2012, the California Attorney General announced an agreement among app platform providers including Amazon, Apple, Google, Hewlett Packard, Microsoft, and Research in Motion, requiring apps in their app stores have privacy policies or disclosures in compliance with California law. The agreement also compelled app store platforms to provide users with a way to report apps that do not comply.

[12] These sign-in boxes often ask users to sign in with personal information like an email account or a social network account like Facebook.

[13] Platforms and application 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.

[14] Users should not have to click through multiple pages and links to access your privacy policy.

When you post a new policy, tell your users upfront what has changed, so they do not have to parse through both the old and new policies to see what is different. Provide a brief statement about the changes with a hyperlink to the old policy for users who want more information.



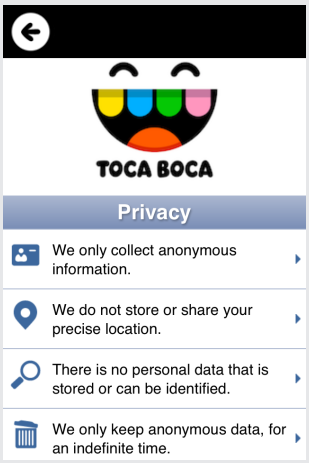
Post updated privacy policies prior to implementing the new data use practices described therein to give your users notice of the change and time to understand them. If you change your data practices, give your users advance notice. For example, posting an updated privacy policy 30 days in advance will give your users time to digest the changes and notify you of any questions or concerns.[15]

If you make material changes to your data policies and practices that will apply to previously-collected data, obtain new permission, i.e. affirmative, opt-in consent, from your users before using that data in new ways.[16]

SHORT-FORM NOTICE

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.

Provide a hyperlink to the full policy in your short-form notice. PrivacyChoice and TRUSTe provide excellent (and sometimes free) tools to help you create your own short-form notices for users.



[15] 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 5-28-12)."

[16] 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 for previously collected data.

ENHANCED NOTICE

Make extra efforts to disclose when you are using sensitive personal information and/or using data in an unexpected way. 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, especially when you are using sensitive data or using data in an unexpected way. Make clear, conspicuous, and timely disclosures when engaging in this use. Take note of the nuances of "unexpected uses" and "sensitive data."

There is no set definition of "unexpected uses" — this determination depends heavily on context.[17] However, these uses might include the following:

- 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 definition of "sensitive" varies from jurisdiction to jurisdiction, but often includes data related to health, finances, race, religion, political affiliation, political 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 users understand this and expressly agree to its use.[18] Sensitive user data warrants stronger protections and often carries specific legal requirements. Simply describing these uses in a privacy policy or terms of use is not sufficient.

1. Sharing Data with Third Parties

Use additional notice to highlight data use practices that involve the transfer of users' data.[19] If your app uses third party analytics or is supported by ads, you are likely collecting or disclosing user information. 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.

[17] In some 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, it may not be obvious to the user why a chess game application would want access to photos and videos.

[18] In certain regulated contexts, various requirements for the exact nature of consent will be applicable.

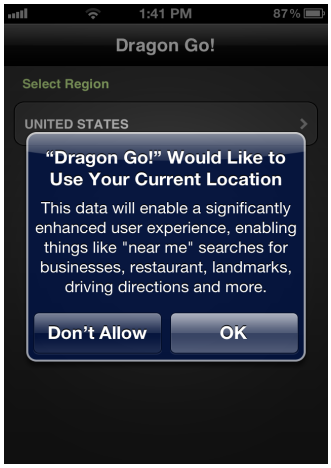
[19] In addition to disclosures made in your comprehensive app privacy policy, you should provide additional notice and disclosure in a short-form notice, the app store description, or permissions once the app is already downloaded and installed.

If you condition the use of your app on the collection and use personal information, educate your users about the trade-off. It's fine to condition distribution of your app on certain data usage, such as sharing personal information with ad networks. However, if your application is a "take it or leave it" deal, make the trade-off clear to users so they understand the exchange. Users may be happy to share their personal information in exchange for your app. However, you need to be transparent and up front in your explanation. Also, note that while it may be appropriate for apps in the U.S. to require consent to "tracking" in exchange for offering users a service, this practice may soon be prohibited in Europe under recently proposed legislation.

Provide notice when sharing location information with third-party advertisers. It may not be obvious to users if you are sharing location information with third-party advertisers. In this 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."

2. Location

Obtain user permission before accessing location data. Precise geo-location information is increasingly considered sensitive information. 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.[20]

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.

The CTIA Best Practices and Guidelines are a useful resource for app developers with mobile applications that use location-based services.

3. Camera

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.[21] Since users are not always aware this is happening, provide notice explaining that geo-tagging may occur.

[20] Some app store platforms have already started to require opt-in consent for access to location data. For example, Apple's App Developer Review Guidelines state: "Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected." (Section 4.1)

[21] Geo-tagging has raised many privacy concerns. Developers may also choose to inform users that they can turn geo-tagging off by shutting down location services prior to taking photos on the device.

4. Automatic Sharing

Many social platforms now enable "frictionless" or social sharing, a way for users to automatically share information with other platform users with minimal steps and effort. 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.[22]

Control & Choice

INDIVIDUAL CHOICE

Give users choice and control around the unexpected collection, storage, or transfer of personal information where feasible. 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.[23]

Provide users with meaningful controls like opt-outs where feasible, particularly when the data is sensitive or used in a non-obvious way.

Allow your users access to the data you keep about them or their device, when possible. If you are keeping records on your users, set up a mechanism so that users can see what information you are collecting and storing about them. If you are transmitting data to third parties, such as ad networks, you should select partners that also offer reasonable access to user files. Access to such data is legally required in many jurisdictions, such as the European Union.

Also, you should strive to ensure that the user's 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.

You may not need to offer choice when the collection and use of the data is reasonably obvious to users.[24] The FTC recently stated that companies do not necessarily have to offer users choice for "commonly accepted" data usages, such as product fulfillment, first-party analytics, security, and accounting and back-office operations.[25] However, if you're unsure whether or not to offer controls in a particular context, it's safer to just provide them.

Regardless of whether you obtain consent from users for specific data uses, you should still describe all data practices in your privacy policy.

---

[22] For example, Facebook apps can only publish user watch and read actions after someone engages with the content for at least 10 seconds. Facebook apps must also clearly inform users that the app will publish these actions on a user's behalf each time a user clicks on a link.

[23] 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 legislative developments in this area.

[24] Note that in some jurisdictions, regulators may require consent for anything other than purposes that are essential for the operation of the app.

[25] Prepared Statement of the FTC on Internet Privacy: The Views of the FTC, the FCC, and NTIA Before the Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, and Subcommittee on Communications and Technology, United States House of Representatives on July 14, 2011 at 14.

TIMING & VISIBILITY

Provide choices to users at the moment and manner in which the notice would be most relevant to the user, within the OS design framework. This usually means before data is accessed, collected and transmitted or used. For example, your app's privacy policy should be accessible before users download the app and/or before prompting users to register, create an account, or use social network information to log in to your app.

Have respect for context. You need to understand and respect the context in which you are collecting and using information. If you process financial data, consumers will obviously hold you to a higher standard than if you collect data related to an app that does not process sensitive information. Timing and visibility is especially important in circumstances that require enhanced notice.[26] Provide users with choice and additional notice or consent mechanisms when your app accesses sensitive information, or when it accesses data/features that may not be obvious to the user. Explain to your users why you need access to such data where feasible.

LIMITATIONS

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. The use of device identifier for tracking as a cookie alternative has created concerns since the identifier cannot be cleared easily.[27] Device identifiers alternatives are currently being debated. Ideally, any identifier used would not be linked directly to the user's identity and would either give the user the ability to clear the identifier or easily opt-out.[28]

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. Although Do Not Track standards have not yet been developed for the mobile app environment, they may be forthcoming.[29] 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.

[26] See Enhanced Notice section in Notice & Transparency on page 6.

[27] The iOS device identifier cannot be cleared at all. Google's Android ID can be cleared but requires a device re-set.

[28] We encourage platforms to 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 Ad Mob 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.

[29] Note that in the FTC's Final Privacy Report, the FTC called for an effective Do Not Track system that would opt users "out of the collection of behavioral data for all purposes other than those that would be consistent with the context of the interactions" with exceptions that may include preventing click-fraud or collecting de-identified data for analytics purposes. http://www.ftc.gov/opa/2012/03/privacyframework.shtm

WHAT DO THE APP STORE PLATFORMS REQUIRE?

As a developer, it's important to understand what a platform requires from you. Different app stores have different 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)

Children

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 under the age of thirteen. Do not request that kind of information unless you have a parent's consent first. You should also avoid sharing information with ad networks for the purpose of behavioral advertising or any other party. 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 with great care. The FTC is reviewing COPPA's scope and applicability to app developers, and youth online privacy is a hot-button issue with legislators, regulators, and the press. The FTC recently proposed to expand the coverage of its protection and expand the definition to personal information.[30] Under the proposed definition, you would have to comply with COPPA if your app is aimed at children and you use a unique identifier (even if that identifier is only used for internal operations such as fraud, first party ads, and maintaining user settings, etc.).

Any app aimed at minors will likely face significant scrutiny, so keep your data collection to an absolute minimum. 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.[31]

[30] FTC Proposed COPPA Rule. http://ftc.gov/opa/2011/09/coppa.shtm

[31] See FTC Staff Report titled, "Mobile Apps for Kids: Current Privacy Disclosures are Dis-appointing." The report also called on app stores to provide a more consistent way for developers to display more information about data collection practices and interactive features on the app. http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

Data Retention & Security

LIMITED DATA COLLECTION & RETENTION

Don't access or collect user data unless your app requires it. 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 even regulators. Delete data that does not need to be retained for a clear business purpose.

Limit the amount of time sensitive data is linked with the user's identifier. Only store sensitive data (such as precise location coordinates) with a unique identifier for the time frame required to operate your app and deliver a service to your users.[32]

Have a data retention policy in place to get rid of user data that you no longer need after a set time period. Don't keep user data indefinitely on the off-chance that it may be valuable someday. This applies whether you store user data on the device, your own servers, or in a cloud platform. Remember to clear associated metadata or cross-references to deleted data. Observing these practices respects your users' privacy interests and helps protect both 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, de-identification of the data may be sufficient if there is no reasonable likelihood that the data can be re-identified, i.e. 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.

Delete user data promptly following the deletion of an account. Users should rightly expect that once they close their account, all their data will be deleted from your server, subject to any legal retention limits.

[32] Subject to legal retention limits.

SECURITY MEASURES

Understand the security risks associated with your app such as the sensitivity of any information you collect and store and the number of people using the app. All applications that access, use, or transfer individuals' data should be tested rigorously for security purposes and comply with current security best practices. Implementing data retention policies and security measures will help ensure user data is properly safeguarded.

1. Encryption

Encrypt data in transit (e.g., use 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 insecure 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.

2. De-Identification

Make efforts to de-identify user data before sharing it with another party. De-identified data is that which cannot be linked to a particular individual through reasonable means. This often involves scrubbing the identifiable elements of personal data, making it comparatively safe in privacy terms, while attempting to retain much of its commercial and scientific value. In its Privacy Report, the FTC provided that personal data may be considered de-identified where, "(1) a given data set is not reasonably identifiable; (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form."[33]

Consider hashing device IDs. Hashing is an encryption technique that uses a cryptographic hash function that transforms data of arbitrary length to a value of a fixed length referred to as the hash value.

3. User Authentication

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.

[33] FTC Privacy Report at 22. http://www.ftc.gov/opa/2012/03/privacyframework.shtm

Accountability

RESPONSIBILITY

Make sure someone is responsible for thinking about 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 must:

- Review your privacy policy before each app release to ensure that it remains accurate and complete,
- Keep an archive of your privacy policy, and ensure that change notices are appropriately posted for users,
- 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,
- Answer all privacy-related emails and communication, and
- Stay on top of new developments by following the FTC and other industry organizations.

PRIVACY BY DESIGN

Practice Privacy by Design. Privacy should be a central consideration in 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.

USER FEEDBACK

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, a feedback forum, or by providing an email address where your users can contact you. Consider highlighting common privacy and security issues in your "Help" or "Settings" page.

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.

Applicable Laws & Regulations

Make sure you comply with applicable laws and regulations. In the United States, federal and state privacy laws only provide protection for certain types 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 any apply to your product or service, conduct further research and/or seek out legal advice. You are responsible for compliance with all applicable laws.

- **Federal Trade Commission "Unfair and Deceptive" Authority**

The Federal Trade Commission (FTC) has general authority to police "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.

- **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 (HIPAA)**

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.

- **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.

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 the law, instead of the 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.

Stay Informed

Stay informed of new developments. New privacy rules and policies are developing quickly. As a developer, you should stay abreast of changes in related regulation and policy matters, as well as new developments that concern apps, such as Do Not Track and device identifier issues.

Resources

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

www.futureofprivacy.org

www.cdt.org