PRIVACY ON THE GO

RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM

January 2013

Kamala D. Harris, Attorney General
California Department of Justice

Table of Contents

Message from the Attorney General

California is the epicenter of modern innovation. Whether in the information technology sector, the entertainment industry, or the development of sustainable energy, the technologies that we create are transforming the world. California has proudly led these innovations, not just by producing new technologies, but also by ensuring that these innovations are used responsibly. In California, we have some of the strongest consumer protection laws in the country. While it is easy to conceive of innovation and regulation as mutually exclusive, California is proof that we can do both. We can innovate responsibly.

The world has gone mobile. Today, 85 percent of American adults own a cell phone and over half of them use their phones to access the Internet. The mobile app marketplace is also booming with more than 1,600 new mobile apps being introduced every day. These apps allow us to do everything from streaming movies to hailing a cab to viewing our own X-ray and ultrasound images.

Along with the many wonderful capabilities these apps offer, we remain mindful that the mobile environment also poses uncharted privacy challenges, such as the difficulty of providing consumers with meaningful information about privacy choices on small screens and the many players who may have access to sensitive user information. These are challenges that we must confront and that we must resolve in a way that appropriately protects privacy while not unduly stifling innovation. As Attorney General, I am tasked with ensuring that this balance is maintained.

Last year, we took a first step in addressing these challenges with a Joint Statement of Principles that was adopted by the leading operators of mobile application platforms. That agreement improves consumer privacy protections and is designed to help bring mobile apps in compliance with the California Online Privacy Protection Act. As a result of the app platform companies' implementation of the principles, consumers can now review an app's privacy policy in the app store, before downloading the app.

We are now offering this set of privacy practice recommendations to assist app developers, and others, in considering privacy early in the development process. We have arrived at these recommendations after consulting a broad spectrum of stakeholders: mobile carriers, device manufacturers, operating system developers, app developers, app platform providers, mobile ad networks, security and privacy professionals, technologists, academics, and privacy advocates. We are grateful for their comments and look forward to working with all stakeholders in promoting and adopting these recommendations. It is my hope that our recommendations along with continued private-public collaborations will contribute to improving privacy practices in the mobile marketplace.

Sincerely,

Attorney General Kamala D. Harris

This page intentionally left blank

Executive Summary

The pocket computers we carry with us – our cell phones, tablets and such – not only allow us to entertain ourselves, but with nearly a million applications available today, they also offer a variety of other capabilities. Mobile applications (apps) allow us not just to read books, play games, listen to music, and take photos and videos, but also to monitor our heart rate, start the car remotely on a dark night, find a nearby restaurant, and pay for purchases on-the-spot.

With their expanding functionality, mobile devices are subject to the privacy risks of the online world and to some that are unique to the mobile sphere. Their small screen size makes communicating privacy practices and choices to consumers especially challenging. Consumers care about mobile privacy: a recent survey found that over half of Americans had uninstalled or decided not to install an app because of concerns about its privacy practices.[1]

As part of a larger initiative aimed at improving privacy protections in the mobile sphere, the California Attorney General began by forging an agreement with the major app platform companies: Amazon, Apple, Google, Hewlett-Packard, Microsoft, Research In Motion, and later Facebook.[2] These app platform companies agreed to principles designed to improve privacy protections in the mobile environment and to bring the industry in line with California law requiring mobile apps that collect personal information to have a privacy policy. The principles include making an app's privacy policy available to consumers on the app platform, before they download the app.

The mobile app industry is growing fast, but it is still in the early stages of development, with practitioners who are not all alert to privacy implications and how to address them. To help educate the industry and promote privacy best practices, the Attorney General's Privacy Enforcement and Protection Unit has prepared *Privacy on the Go: Recommendations for the Mobile Ecosystem*. The recommendations, which in many places offer greater protection than afforded by existing law, are intended to encourage app developers and other players in the mobile sphere to consider privacy at the outset of the design process.

Recognizing that the legally required general privacy policy is not always the most effective way to get consumers' attention, *Privacy on the Go* recommends a "surprise minimization" approach. This approach means supplementing the general privacy policy with enhanced measures to alert users and give them control over data practices that are not related to an app's basic functionality or that involve sensitive information.

---

[1] Boyles, Jan Lauren, Aaron Smith, Mary Madden, Privacy and Data Management on Mobile Devices. Pew Internet & American Life Project, September 5, 2012, http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx.

[2] See http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

Highlights of Recommendations

For App Developers

- Start with a data checklist to review the personally indentifiable data your app could collect and use it to make decisions on your privacy practices.
- Avoid or limit collecting personally indentifiable data not needed for your app's basic functionality.
- Develop a privacy policy that is clear, accurate, and conspicuously accessible to users and potential users.
- Use enhanced measures – "special notices" or the combination of a short privacy statement and privacy controls – to draw users' attention to data practices that may be unexpected and to enable them to make meaningful choices.

For App Platform Providers

- Make app privacy policies accessible from the app platform so that they may be reviewed before a user downloads an app.
- Use the platform to educate users on mobile privacy.

For Mobile Ad Networks

- Avoid using out-of-app ads that are delivered by modifying browser settings or placing icons on the mobile desktop.
- Have a privacy policy and provide it to the app developers who will enable the delivery of targeted ads through your network.
- Move away from the use of interchangeable device-specific identifiers and transition to app-specific or temporary device identifiers.

For Operating System Developers

- Develop global privacy settings that allow users to control the data and device features accessible to apps.

For Mobile Carriers

- Leverage your ongoing relationship with mobile customers to educate them on mobile privacy and particularly on children's privacy.

I. Introduction

The Movement to Mobile

Mobile devices are integral to modern life and their use is growing rapidly. Today, 85 percent of American adults have a cell phone, 45 percent a smart phone, 61 percent a laptop, 25 percent a tablet computer, and 18 percent an e-book reader. Over half of adult cell phone owners use the Internet on their phones, twice the rate in 2009. And nearly one third of cell owners report that their phone is the primary, or only, way they access the Internet.[1]

The ever-expanding capabilities of mobile devices have created an exploding market for applications (apps) that allow us not just to read books, play games, listen to music, and take photos and videos, but also to monitor our heart rate, start the car remotely on a dark night, find a nearby restaurant, and pay for purchases on-the-spot. Recent reports estimate that there are more than a million apps available on the primary mobile platforms, and more than 1,600 new apps are added daily.[2]

Clearly, many consumers find value in mobile apps and are eager to try new ones as they are released. But many of these same consumers are also concerned about privacy. A recent study found that more than half of mobile app users had uninstalled or decided not to install an app because of concerns about its privacy practices.[3] Addressing these concerns is essential to protect consumers and to foster trust and confidence in this market.

Mobile Privacy Issues

Our smart phones and other mobile devices are pocket computers. They now have the power and functionality of desktop computers – and the privacy and security risks inherent to the Internet. Like our desktop and laptop computers, our mobile devices may contain, or are capable of accessing, large amounts of personal information: contact information of our friends and associates, family photos and videos, and our web browsing history, among other details. And like personal computers, smart phones, and other mobile devices are targets for malware and spyware.[4]

These always-on, always-on-us devices pose additional privacy challenges that are unique to the mobile space. Mobile devices may store types of user information not usually found on personal computers, such as telephone call logs, text messages, and a history of our location. Mobile devices and apps are also leading to new forms and combinations of user and device-related data that may pose new risks to users' privacy and security.

Another challenge is the devices' small screens, which make the effective communication of privacy practices and user choices difficult. Furthermore, although the app economy is thriving, the mobile app industry is in a relatively early development stage, with developers focusing on getting new products to market as quickly as possible, sometimes without adequate consideration of privacy. Recent studies, for example, have found

that many mobile apps did not provide users with privacy policy statements at all.[5] This represents not just a failure in transparency, but it also suggests a lack of attention to the apps' privacy practices.

In an important step to strengthen the privacy protections for users of mobile applications, the California Attorney General in early 2012 announced a Joint Statement of Principles, endorsed by the companies whose platforms comprise the majority of the mobile app market (Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft, and Research In Motion). The principles are intended to ensure that mobile apps comply with applicable privacy laws such as the California Online Privacy Protection Act, and include the conspicuous posting of a privacy policy by mobile apps when required by law, a means to make the policy available from the app platform before downloading, a way for users to report non-compliant apps to the platform provider, a process to respond to such reports, and a pledge to further work with the Attorney General on best practices for mobile privacy.[6] As of October 2012, all the app store companies who joined the agreement reported that they had implemented the principles.

The agreement with the platform providers has already had an impact on privacy practices. A June 2012 study found that the percentage of the most popular apps with some form of access to a privacy policy improved significantly since their similar study in September 2011. In just eight months, free apps on the Apple App Store platform with a privacy policy doubled, from 40 percent to 84 percent, and those on the Google Play platform increased from 70 percent to 76 percent.[7]

Recommended Practices

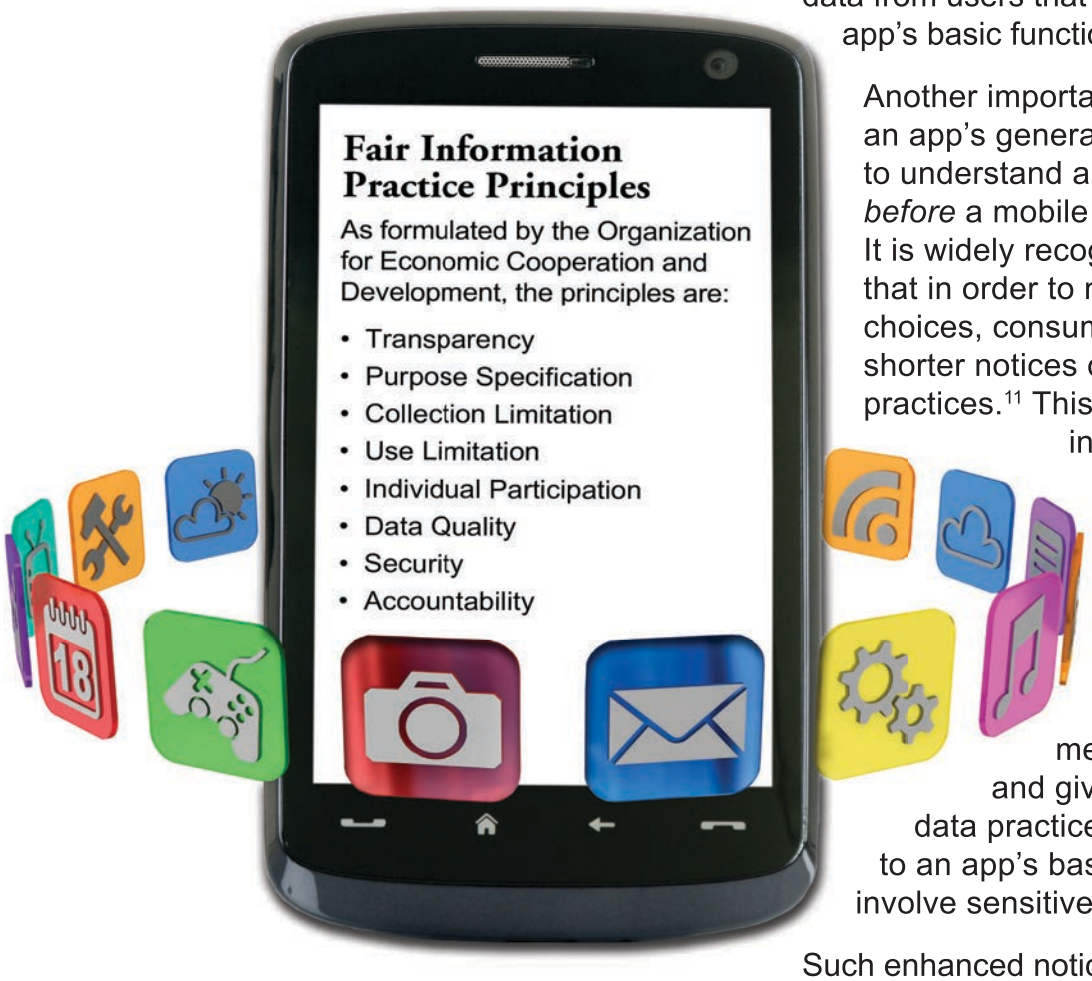
The Attorney General is committed to increasing compliance with California's privacy laws. In July 2012, the Attorney General created the Privacy Enforcement and Protection Unit, with the mission of protecting the inalienable right to privacy conferred by the California Constitution. The Privacy Unit enforces state and federal privacy laws, and develops programs to educate consumers and businesses on privacy rights and best practices. *Privacy on the Go* is part of the effort to encourage businesses to adopt privacy best practices.

Several respected organizations have recently issued privacy principles and policies for the mobile industry.[8] The shared themes of these sets of principles have informed our recommended practices: transparency about data practices, limits on the collection and retention of data, meaningful choices for users, security, and accountability of all industry actors for privacy.

We offer these privacy practice recommendations to assist the mobile ecosystem in the ongoing efforts to develop privacy standards. Our hope is that privacy-respectful practices such as those we are recommending here will be adopted by app developers and others, enabling consumers to make informed choices from the vast array of mobile apps while maintaining the level of privacy control they desire.

Our recommendations, which in many places offer greater protection than afforded by existing law, are intended to encourage all players in the mobile marketplace to consider privacy implications *at the outset* of the design process. They are also intended to encourage the alignment of architectural and functional decisions

with the widely accepted Fair Information Practice Principles (FIPPs). The FIPPs form the basis for many privacy codes and laws in different parts of the world, including the federal Privacy Act of 1974 and the similar California Information Practices Act of 1977.



Like many actors in the mobile ecosystem, the Attorney General is also participating in the multi-stakeholder process facilitated by the National Telecommunications and Information Administration (NTIA) to develop an enforceable code of conduct on mobile app transparency.[10] While our recommendations engage a broader range of mobile privacy issues than the NTIA is expected to address at this time, we hope that this document will be useful in the ongoing NTIA process.

Surprise Minimization

The basic approach recommended here is to minimize surprises to users from unexpected privacy practices. An obvious way to avoid such unpleasant surprises is to avoid collecting personally indentifiable data from users that are not needed for an app's basic functionality.

Another important step is to make an app's general privacy policy easy to understand and readily available *before* a mobile app is downloaded. It is widely recognized, however, that in order to make meaningful choices, consumers need clearer, shorter notices of certain privacy practices.[11] This is particularly true in the small-screen mobile environment. Our recommended approach is to supplement the legally required general privacy policy with enhanced measures to alert users and give them control over data practices that are not related to an app's basic functionality or that involve sensitive information.

Such enhanced notice and control might be provided through "special notices," delivered in context and just-in-time. For example, operating systems that use location data deliver a notice just before collecting the data and give users an opportunity to allow or prevent the practice.

Another way to achieve the same end is to make readily available from within an app both a short privacy statement highlighting potentially unexpected practices, and privacy controls that allow users to make, review, and change their privacy choices.

Shared Accountability

We are addressing these initial recommendations primarily to app developers, but we include some recommendations to other actors in the ecosystem.

Protecting consumer privacy is a team sport. The decisions and actions of many players, operating individually and jointly, determine privacy outcomes for users. Hardware manufacturers, operating system developers, mobile telecommunications carriers, advertising networks, and mobile app developers all play a part, and their collaboration is crucial to enabling consumers to enjoy mobile apps without having to sacrifice their privacy.

By offering consumers greater transparency and control over how their information is collected and used in the mobile ecosystem, the industry will build the trust that is critical for the app market to flourish.

Key Terms

The following definitions are for key terms as they are used in this document.

Personally indentifiable data are any data linked to a person or persistently linked to a mobile device: data that can identify a person via personal information or a device via a unique identifier. Included are user-entered data, as well as automatically collected data.

Sensitive information is personally indentifiable data about which users are likely to be concerned, such as precise geo-location; financial and medical information; passwords; stored information such as contacts, photos, and videos; and children's information.

Special notice is a timely, contextual notice that alerts users to a data practice that is likely to be unexpected because it involves sensitive information or data not required for an app's basic functionality.

Short privacy statement is a privacy policy designed to be read on a mobile device, highlighting data practices that involve sensitive information or are likely to be unexpected because they involve data not required for an app's basic functionality.

Privacy controls are settings available within an app or an operating system that allow users to make or revise choices offered in the general privacy policy about the collection of their personally indentifiable data.

General privacy policy is a comprehensive statement of a company's or organization's policies and practices related to an application, covering the accessing, collecting, using, disclosing, sharing, and otherwise handling of personally indentifiable data.

Acknowledgements

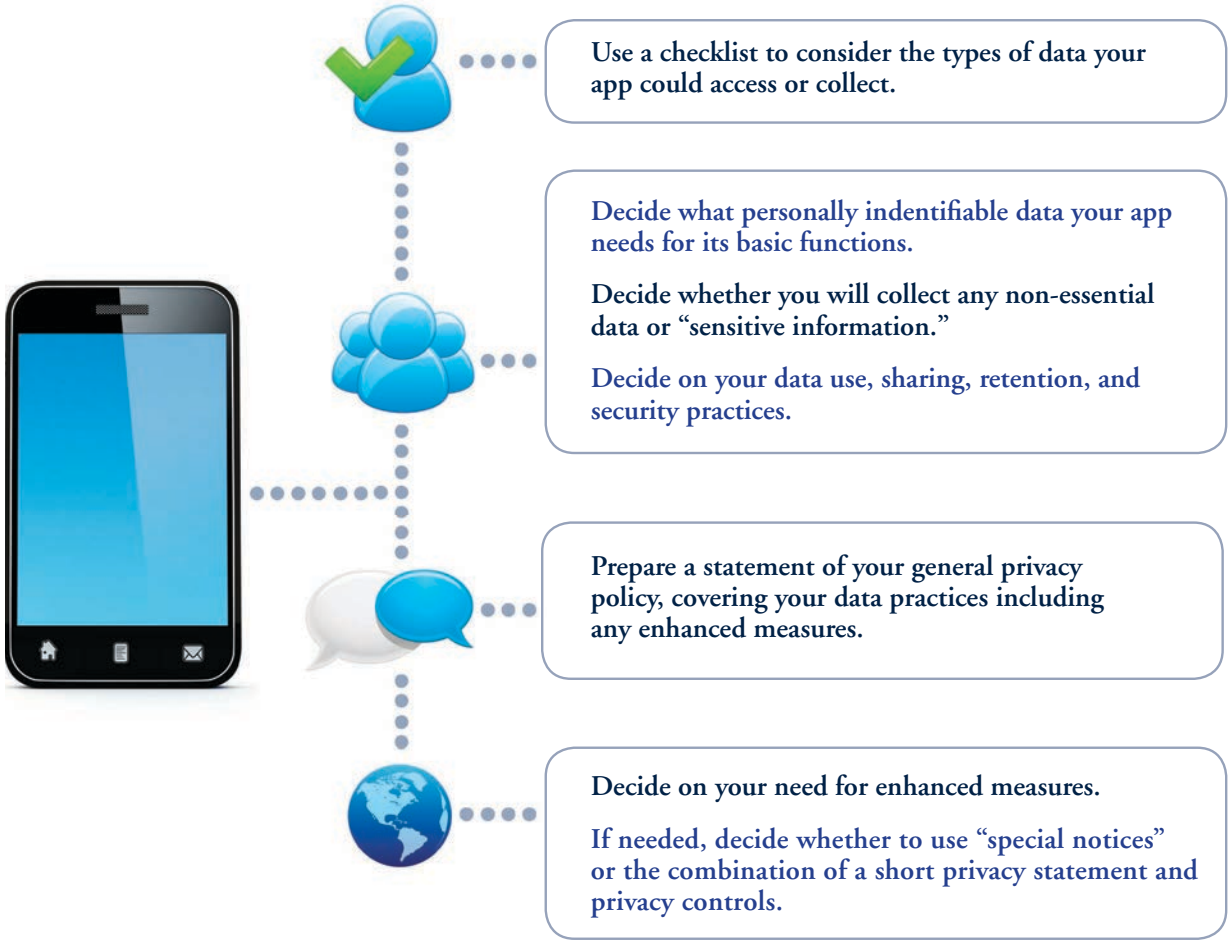
In developing our recommendations we benefited from the advice of a broad spectrum of stakeholders: mobile carriers, device manufacturers, operating system developers, app developers, app platform providers, mobile ad networks, security and privacy professionals, technologists, academics, and privacy advocates. Their comments and contributions are greatly appreciated.

II. Recommendations for App Developers

The app economy in the U.S. is estimated to account for 466,000 jobs, up from zero in 2007 when the iPhone was introduced.[12] The burgeoning mobile app industry is primarily made up of small businesses, often individual developers, whose newly formed industry associations have expressed a commitment to respect the privacy of their users.[13] We offer these recommendations to help in the development of privacy standards for the mobile app industry.

In this section, we discuss ways that developers can build privacy into their apps. We begin by encouraging the use of a data checklist, which can be used in making decisions about privacy practices, in designing an app, and in generating privacy notices and statements. We go on to discuss certain practices that are intended to minimize unpleasant surprises for users, and we offer recommendations on the general privacy policy and on enhanced privacy measures to supplement it.

Decision Path for Building Privacy into Apps



Start with a Data Checklist

The most efficient way to build privacy into an app is to consider it at the outset of the development process. App developers should also consider privacy when making updates in technology and business practices.

As a first step, create a checklist to assess your app's potential collection, use, and disclosure of personally indentifiable data. The checklist will facilitate design and privacy practice decisions that reduce risks for both you and your users. A checklist is also useful in preparing a general privacy policy, special notices, and privacy controls.

Consider the Data

Consider the personally indentifiable data[14] your app may collect, use, or disclose to third parties. You should also consider the data collection and use practices of any third-party software (such as libraries or SDKs) used in your app. This may require testing, as well as reading about the third-party software's data collection practices.[15] Types or categories of personally indentifiable data include the following:

- Unique device identifier
- Geo-location (GPS, WiFi, user-entered)
- Mobile phone number
- Email address
- User's name
- Text messages or email
- Call logs
- Contacts/address book
- Financial and payment information
- Health and medical information
- Photos or videos
- Web browsing history
- Apps downloaded or used

Create a Checklist

Use a checklist or matrix to record the types or categories of personally indentifiable data collected and answer the following questions *for each type of data*:

- Is the data type necessary for your app's basic functionality (that is, within the reasonably expected context of the app's functions as described to users)?
- Is the data type necessary for business reasons (such as billing)?
- How will you use the data?
- Will it be necessary to store data off the device, on your servers?
- How long will you need to store the data on your servers?
- Will you share the data with third parties (such as ad networks, analytics companies, service providers)? If so, with whom will you share it?
- How will third parties use the data?
- Who in your organization will have access to user data?
- Is your app directed to or likely to be used by children under the age of 13?
- What parts of the mobile device do you have permissions to access? Can you provide users with the ability to modify permissions?

Privacy Practices

Once you have used a checklist to consider all the personally indentifiable data that your app could collect, you are ready to make decisions about your privacy practices. These decisions include what data you will collect, how you will use it, how long you will retain it, with whom you will share it, how you will secure it, and what choices you will give your users about their data.

Be Transparent

- Make your privacy practices available to users before the app is downloaded and any data is collected. You can accomplish this is by making your general privacy policy available from the app platform.
- Make your general privacy policy readily accessible from within the app.
- In addition, use enhanced measures to draw users' attention to data practices that may be unexpected or that involve sensitive information.
- Keep your privacy policy communications up-to-date in reflecting your actual data-handling practices.

Limit Data Collection

- Avoid or minimize the collection of personally indentifiable data for uses not related to your app's basic functionality, and limit the retention of such data to the period necessary to support the intended function or to meet legal requirements.
- Avoid or limit the collection of sensitive information.
- If your app is directed to children under the age of 13 or if you know that you are collecting personal information from children under the age of 13, you may have additional obligations under federal law.[16]
- Use an app-specific or other non-persistent device identifier rather than a persistent, globally unique identifier.
- Give users control over the collection of any personally indentifiable data used for purposes other than the app's basic functions.
- The default settings should be privacy protective.
- You may want to explain the consequences of not allowing the collection of the data.

Limit Data Retention

Do not retain data that can be used to identify a user or device beyond the time period necessary to complete the function for which the data were collected or beyond what was disclosed to the user.

- Adopt procedures for deleting personally indentifiable user data that you no longer need.

Give Users Access

- Develop mechanisms to give users access to the personally identifiable data that the app collects and retains about them.

Use Security Safeguards

Use security safeguards to protect personally indentifiable data from unauthorized access, use, disclosure, modification, or destruction. Safeguards should include, but not be limited to, the following:

- Limit access to personally identified user data by those inside your organization to a need-to-know basis.
- Use encryption in the transit and storage of personally indentifiable data.
- If you collect payment card information, comply with the Payment Card Industry Data Security Standard.[17]
- Work with others in the ecosystem to ensure the application of appropriate security measures to protect personally indentifiable data.

Be Accountable

- You are accountable for complying with applicable laws and with your general privacy policy and any privacy notices you provide.
- Make someone in your organization responsible for reviewing your general privacy policy whenever the app is updated or your business practices change. This person should also maintain an archive of previous versions of the policy, confirm your rules for limiting internal access to personally indentifiable user data, act as the point of contact for privacy questions and comments, and stay informed of new privacy laws and regulations.
- Ensure that all who work in your organization receive training in privacy obligations and in your own policies and practices. Such training should be provided at least annually and to new employees as they are hired.
- In addition to state and federal privacy laws, international jurisdictions have data protection laws that may apply to the data collection practices of your app.

General Privacy Policy

When you have decided on the privacy practices you will use in your app, you are ready to describe them in a general privacy policy. The policy should provide a comprehensive overview of your practices, and should comply with legal requirements for such policies.[18] The following recommendations are intended to make your general privacy policy statement more effective and meaningful in providing transparency about your data practices.

Make It Easy to Find

- Make the privacy policy conspicuously accessible to users and potential users.[19]
- Post or link the policy on the app platform page, to make it available to users before the app is downloaded.[20]
- Link to the policy within the app (for example, on controls/settings page). Consider hosting the privacy policy in the browser to facilitate updates in case your practices change.[21]

Make It Easy to Read

- Make the privacy policy clear and understandable by using plain language and a format that is readable on a mobile device.
    - One format is a layered notice that highlights the most relevant privacy issues.[22]
    - Another format is a grid or "nutrition label for privacy" that displays your privacy practices by data type.[23]
- Graphics or icons can help users to easily recognize privacy practices and settings.
    - Privacy icons will be most effective if they are widely used and consumer comprehension is supported by an awareness campaign.[24]

Describe Your Practices

The privacy policy should describe your practices regarding the collection, use, sharing, disclosure, and retention of personally indentifiable data, including at least the following items:

- The types or categories of personally indentifiable data collected by the app.[25]
- The uses and retention period for each type or category of personally indentifiable data.
- Whether your app, or a third party, collects payment information for in-app purchases.
- The categories of third parties with whom the app may share personally indentifiable data.[26] Such third parties include advertising networks and analytics providers. Provide a link to third parties' privacy policy statements, where available.
- The choices a user has regarding the collection, use, and sharing of user information, with instructions on how to exercise those choices.
- The process for a user to review and request corrections to his or her personally identifiable information maintained by the app, if available.[27]
- A means for users to contact the app developer with questions or concerns.
- The effective date of the privacy policy and the process for notifying users of material changes to it.[28]

Enhanced Measures

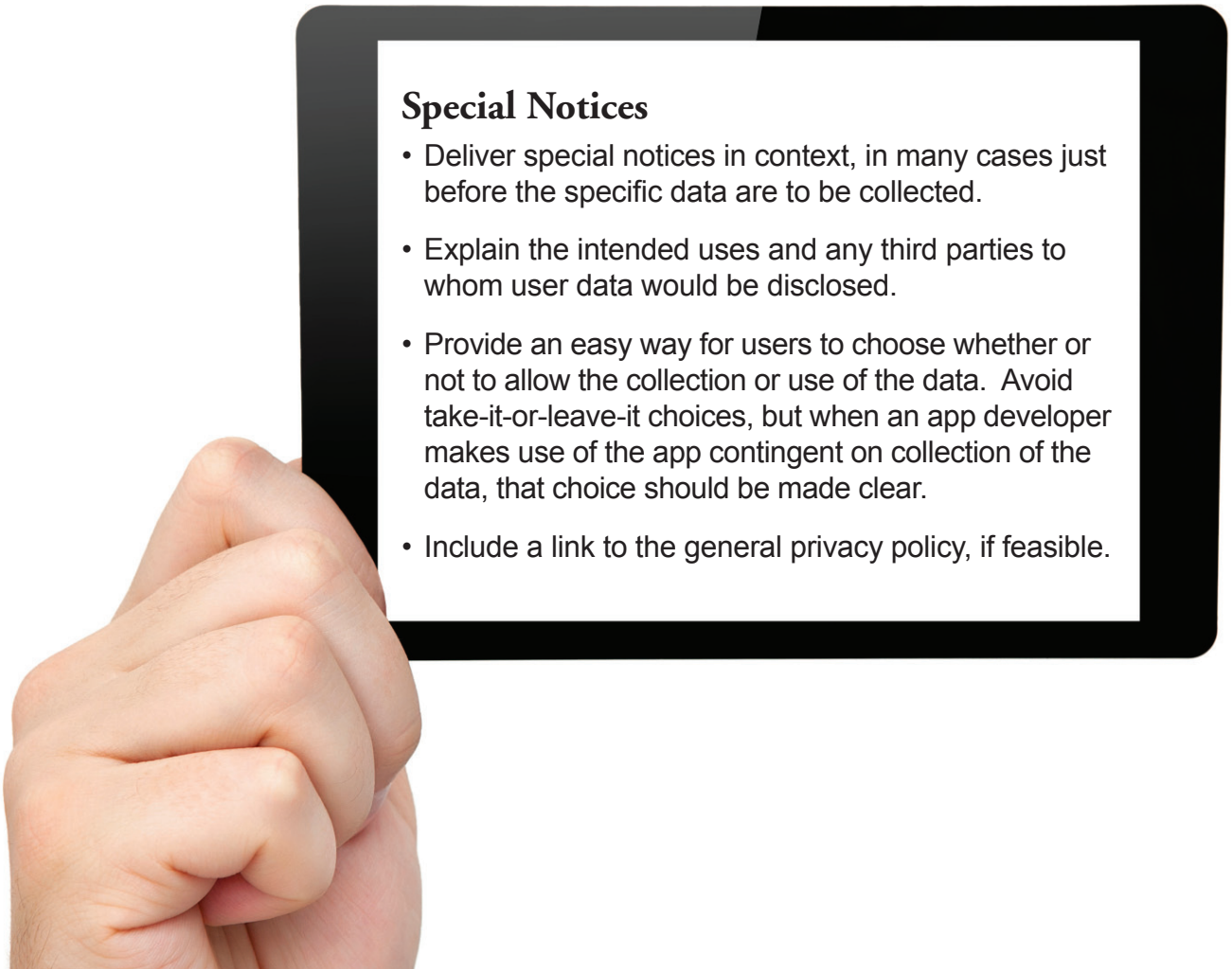
If your app collects sensitive information or personally indentifiable data not needed for its basic functionality, then supplement your general privacy policy with enhanced measures to alert users.

Special Notices

One way to do this is through the use of "special notices."[29]

Practices that are likely to deserve special notice include the following:

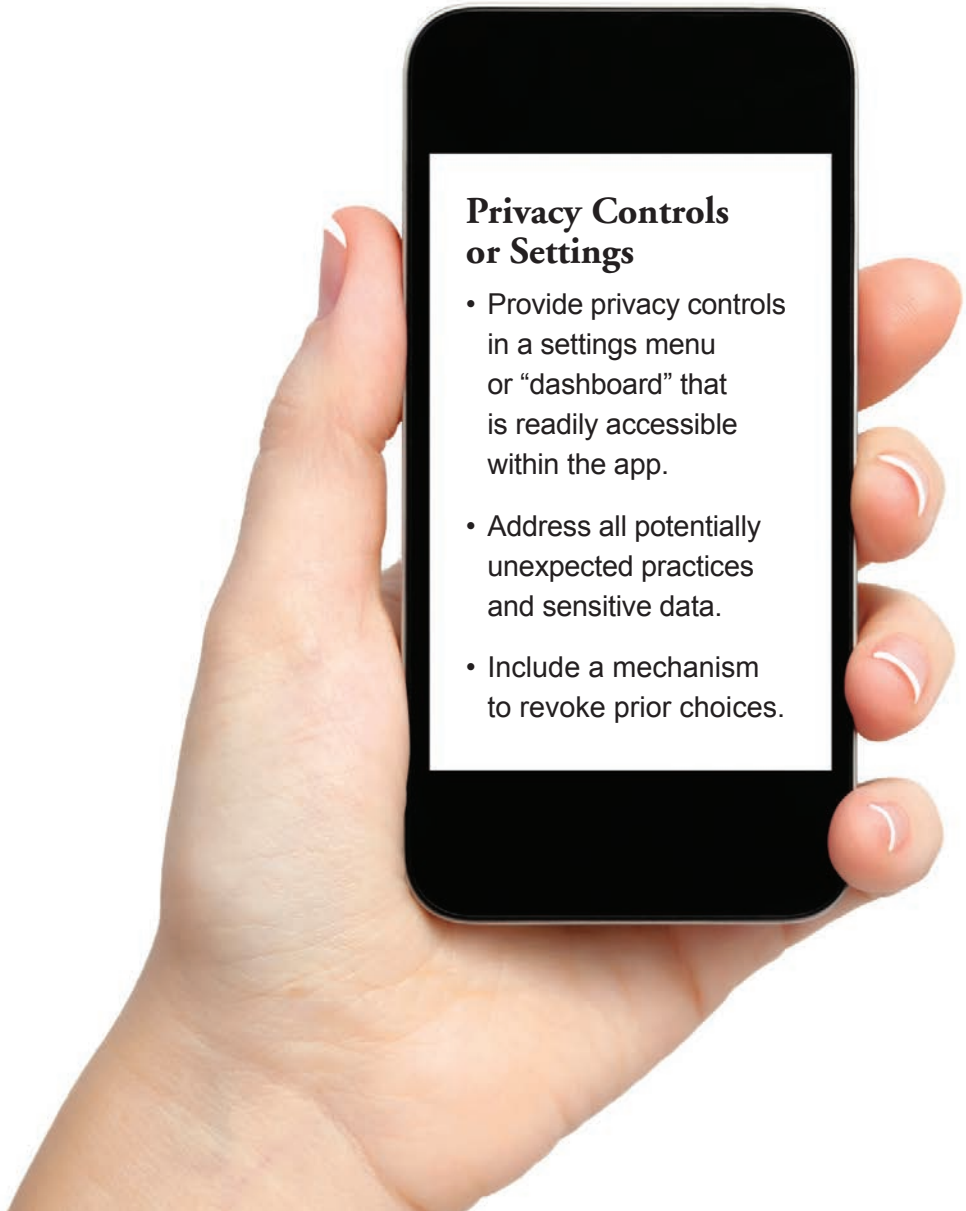
- Collection, use or disclosure of personally indentifiable data not required for your app's basic functionality.[30]
- Accessing text messages, call logs, contacts or potentially privacy-sensitive device features such as camera, dialer, and microphone.
- A change in your data practices that involves new, unexpected uses or disclosures of personally indentifiable data.[31]
- The collection or use of sensitive information (such as precise geo-location, financial or medical information, passwords).
- The disclosure to third parties of personally indentifiable information for their own use, including use for advertising.



Short Privacy Statement and Privacy Controls

Another approach is to use the combination of a short privacy statement and privacy controls.

- The short privacy statement should highlight the potentially unexpected practices and sensitive information discussed above under Special Notices.
- Readily accessible privacy controls should give users a convenient way to make choices and to change them when desired. The operating system may provide such controls.



III. Recommendations for App Platform Providers

In the Joint Statement of Principles of February 2012, the major app platform providers (Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft, and Research In Motion) and the California Attorney General agreed to certain practices to increase consumer privacy protections in the mobile marketplace.[32] In addition, the platform providers pledged to work with the Attorney General on best practices for mobile privacy in general. The following recommendations are offered as a step in the development of such best practices.

In this section, we encourage platform providers to use their pivotal role to improve privacy practices and privacy understanding among developers and consumers.

Privacy Practices

- Give consumers an opportunity to learn about an app's privacy practices before downloading the app by making app developers' general privacy policy conspicuously accessible to users and potential users on the app platform.
- Educate app developers about their obligations to respect consumer privacy and disclose to consumers what personally identifiable information they collect, how they use the information, with whom they share it, and other privacy practices.
- Provide app users with tools to report apps that do not comply with applicable laws, or their privacy policies or terms of service about which they have questions.
    - Make it easy for users to find out how to contact you about apps, such as through a link on the app platform page.
    - Implement processes to respond to these reports.
- Help to educate consumers on mobile privacy.
    - Provide educational information on or linked from the app platform.
    - Encourage consumers to review the app privacy policy before downloading an app.
    - Encourage consumers to look for privacy choices and controls in apps after downloading.
    - Inform parents of resources available to help protect their children's privacy, such as the FTC's information for parents on the Children's Privacy Protection Act.[33]

IV. Recommendations for Advertising Networks

A common business model for mobile apps today is based on delivering targeted advertising to app users.[34] The collection of user information is enabled by the app, with the related data flows remaining largely invisible to users. Ad networks should provide app developers with clear, comprehensive information on their privacy practices.

In this section, we offer recommendations intended to help establish privacy practices for in-app mobile ad technologies. The recommendations address transparency and increased user control over the use of personally indentifiable data by third parties for purposes of behavioral advertising.[35]

Privacy Practices

- Prepare a privacy policy that describes your collection, use, disclosure, and retention of personally indentifiable user data. See the recommendations for app developers in Section II for more on what to include at a minimum in your general privacy policy.
- Provide your privacy policy to the app developers who will enable the delivery of targeted ads through your network. Provide a link to your privacy policy for app developers to make available to users before they download and/or activate the app.
- Provide clear information on the impact of your practices on app SDKs.
- Avoid delivering ads outside the context of the app. Examples are delivering ads by modifying browser settings or placing icons on the mobile desktop.
    - Use enhanced measures and obtain prior consent from users before delivering out-of-app ads. (See Section II.)
    - When delivering out-of-app ads, provide clear attribution to the host application responsible.
- Use enhanced measures and obtain prior consent from users before accessing personal information such as phone number, email address or name. (See Section II.)
- Move away from the use of unchangeable device-specific identifiers and transition to using app-specific and/or temporary device identifiers.
- Transmit user data securely, using encryption for permanent unique device identifiers and personal information, such as an email address or phone number.

V. Recommendations for Others

In this section, we highlight opportunities for collaboration among other players in the mobile ecosystem.

Operating System Developers

- Work with mobile carriers and other appropriate parties to facilitate timely patching of security vulnerabilities.
- Work with device manufacturers and mobile carriers on setting cross-platform standards for privacy controls, means of enabling the delivery of special privacy notices, and privacy icons.
- Develop global privacy settings and overrides that users can use to set controls for personally indentifiable data, features or hardware configurations that can be accessed by apps.
- Provide tools for app developers that enable comprehensive evaluation of data collection, use and transmission.

Mobile Carriers

- Leverage your ongoing relationship with your mobile customers to educate them on privacy protection.
    - Encourage consumers to review the app privacy policy statement before downloading an app.
    - Encourage consumers to look for privacy choices and controls in apps after downloading.
    - Help to educate parents on mobile privacy and safety for their children. Consider, for example, providing information on available resources, such as the FTC's information for parents on the Children's Privacy Protection Act.[36]
- Work with operating system developers and other appropriate parties to facilitate timely patching of security vulnerabilities.
- Work with operating system developers and device manufacturers on setting cross-platform standards for privacy controls, means of enabling the delivery of special privacy notices, and privacy icons.

Appendix: California Online Privacy Protection Act[37]

Business and Professions Code Sections 22575-22579

22575. (a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(b) The privacy policy required by subdivision (a) shall do all of the following:

(1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.

(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.

(4) Identify its effective date.

22576. An operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service and who reside in California shall be in violation of this section if the operator fails to comply with the provisions of Section 22575 or with the provisions of its posted privacy policy in either of the following ways:

(a) Knowingly and willfully.

(b) Negligently and materially.

22577. For the purposes of this chapter, the following definitions apply:

(a) The term "personally identifiable information" means individually indentifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

(1) A first and last name.

(2) A home or other physical address, including street name and name of a city or town.

(3) An e-mail address.

(4) A telephone number.

(5) A social security number.

(6) Any other identifier that permits the physical or online contacting of a specific individual.

(7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

(b) The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:

(1) A Web page on which the actual privacy policy is posted if the Web page is the home page or first significant page after entering the Web site.

(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the home page or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.

(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the home page or first significant page after entering the Web site, and if the text link does one of the following:

(A) Includes the word "privacy."

(B) Is written in capital letters equal to or greater in size than the surrounding text.

(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.

(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.

(c) The term "operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.

(d) The term "consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.

22578. It is the intent of the Legislature that this chapter is a matter of statewide concern. This chapter supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the posting of a privacy policy on an Internet Web site.

22579. This chapter shall become operative on July 1, 2004.

Notes

[1] Brenner, Joanna. Pew Internet: Mobile. Pew Internet & American Life Project, December 4, 2012, www.pewinternet.org/Commentary/2012/February/Pew-Internet Mobile.aspx.

[2] New apps are being added at the rate of 746 per day for Apple App Store, 665 for Google Play, 181 for Windows Marketplace, and 75 for Amazon Appstore, according to an August 19, 2012 report in *ConceivablyTech*, available at www.conceivablytech.com/10283/business/apple-app-store-to-reach-1m-apps-this-year-sort-of.

[3] Boyles, Jan Lauren, Aaron Smith, Mary Madden, Privacy and Data Management on Mobile Devices. Pew Internet & American Life Project, September 5, 2012, pewinternet.org/Reports/2012/Mobile-Privacy.aspx.

[4] See Lookout Mobile Security's report, State of Mobile Security 2012, available at https://www.lookout.com/resources/reports/state-of-mobile-security-2012.

[5] See Your Apps Are Watching You, *Wall Street Journal* (December 17, 2010); Federal Trade Commission, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (February 2012); Federal Trade Commission, Mobile Apps for Kids: Disclosures Still Not Making the Grade (December 2012); and Future of Privacy Forum, FPF Mobile Apps Study (June 2012).

[6] The Joint Statement of Principles and related information may be found at www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy. The California Online Privacy Protection Act, included in the Appendix to this document, requires operators of commercial websites or online services that collect personal information from Californians to conspicuously post a privacy policy and to comply with its policy. The policy must, among other things, identify the categories of personally identifiable information collected about site users and the categories of third parties with whom an operator may share the information.

[7] Future of Privacy Forum, June 2012 FPF Mobile Apps Study, available at www.futureofprivacy.org/mobile-apps-study.

[8] See Mobile Privacy Principles (March 2012) from GSMA, the global trade association for the mobile industry, at www.gsma.com/publicpolicy/mobile-privacy-principles, and the Mobile User Privacy Bill of Rights (March 2012), from the Electronic Frontier Foundation, at www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights. Also see Best Practices for Mobile Applications Developers (December 2011), from the Center for Democracy and Technology and the Future of Privacy Forum, at www.cdt.org/blogs/2112best-practices-mobile-applications-developers, and Web Application Privacy Best Practices (July 2012), which covers mobile apps, from the World Wide Web Consortium, at www.w3.org/TR/2012/NOTE-app-privacy-bp-20120703/.

[9] The Principles were first articulated by the U.S. Department of Health Education and Welfare in 1973, in recognition of the impact of the computerization of information on individual privacy interests and intended to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy. In 1980, the Organization for Economic Cooperation and Development codified them in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. While the FIPPs remain central to privacy protection, some privacy scholars have begun to question the adequacy of the traditional approach in the era of Big Data. See, for example, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010), and Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NYU L. Rev. 1814 (2011).

[10] The Federal Register notice of the NTIA process is available at www.ntia.doc.gov/federal-register-notice/2012/notice-privacy-multistakeholder-process-open-meetings.

[11] See Graber, M.A., D'Alessandro, D.M., and Johnson-West, J., Reading level of privacy policies on internet health web sites, *Journal of Family Practice* (July 2002); McDonald, A.M., and Cranor, L.F., The cost of reading privacy policies, *I/S-A Journal of Law and Policy for the Information Society 4*, 3 (2008); Pollach, I., What's wrong with online privacy policies? *Communications of the ACM 30*, 5 (September 2007), 103-108.

[12] TechNet, *Where the Jobs Are: The App Economy* (February 2012), research conducted by Dr. Michale Mandel, South Mountain Economics, LLC, available online at www.technet.org/new-technet-sponsored-study-nearly-500000-app-economy-jobs-in-united-states-february-7-2012/. The total includes jobs at firms dedicated to developing apps, app-related jobs at larger companies, and app "infrastructure" jobs at firms such as Google, Apple, and Facebook.

[13] See the App Developers Alliance, http://appdevelopersalliance.org/policy, and the Association for Competitive Technology, http://actonline.org/.

[14] See definition of "personally indentifiable data" on page 6.

[15] See the design solutions to common privacy problems from the University of California at Berkeley's School of Information, at www.privacypatterns.org.

[16] Consult the Federal Trade Commission's guidance on how to comply with the Children's Online Privacy Protection Act before collecting any such information (http://business.ftc.gov/documents/bus45-how-comply-childrens-online-privacy-protection-rule).

[17] Information on the standard can be found at https://www.pcisecuritystandards.org/security_standards/.

[18] The California Online Privacy Protection Act, Business and Professions Code §§22575-22579, included in the Appendix to this document, requires operators of commercial web sites or online services that collect "personally identifiable information" on California residents to post privacy policies. The Children's Online Privacy Protection Act, 15 U.S. Code § 6501 and following, imposes requirements on operators of commercial web sites or online services directed to children under the age of 13 or that knowingly collect information from children under the age of 13. Also see note 35.

[19] See Business and Professions Code § 22575(a).

[20] See the Joint Statement of Principles between the California Attorney General and the major app platform providers, at www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

[21] See Business and Professions Code § 22577(b)(5).

[22] See www.truste.com and www.privacychoice.org for examples of a layered privacy policy presentation on a mobile device. These models may be useful, but no model privacy policy should be followed without assessing your practices and ensuring that your policy statement reflects your practices accurately.

[23] Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder, A "Nutrition Label" for Privacy, Symposium On Usable Privacy and Security (SOUPS), 2009, Article No. 4, available at http://cups.cs.cmu.edu/privacyLabel/.

[24] For examples of privacy icons, see the set proposed by the Association for Competitive Technology, at http://apptrustproject.com, and Mozilla's privacy icons in beta release, at https://wiki.mozilla.org/Privacy_Icons.

[25] See Business and Professions Code § 22575(b)(1).

[26] See Business and Professions Code § 22575(b)(1).

[27] See Business and Professions Code § 22575(b)(2).

[28] See Business and Professions Code § 22575(b)(3) and (4).

[29] "Special notices" are consistent with the concept of privacy notices delivered in times and places where they are useful to consumers that is encouraged in the White House's *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012) and in the Federal Trade Commission's *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012).For an understanding of when a data practice could be considered "expected," and therefore not needing a special notice, see the FTC report's discussion of the need to consider the context of the interaction between a business and a consumer and their suggestion that practices that are "consistent with

the context of the transaction or the consumer's existing relationship with the business, or are required or specifically authorized by law" would not be unexpected (pages 38-39 of the report cited).

[30] Basic functionality includes support for internal operations. As defined by the FTC in the December 2012 amendments to the Children's Online Privacy Protection Rule, support for the internal operations of the website or online service means those activities necessary to: (a) maintain or analyze the functioning of the website or online service; (b) perform network communications; (c) authenticate users of, or personalize the content on, the website or online service; (d) serve contextual advertising on the website or online service or cap the frequency of advertising; (e) protect the security or integrity of the user, website, or online service; (f) ensure legal or regulatory compliance; or (g) fulfill a request of a user; so long as the information collected for the activities listed in paragraphs (a)-(g) is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose. The text of the Rule is available at www.ftc.gov/opa/2012/12/coppa.shtm.

[31] If you make material changes to your data practices, in addition to updating your general privacy policy statement, use a special notice. The notice should alert users to new collection, use or disclosure of personally indentifiable data. Provide a special notice before implementing the new practice and get user consent before applying it to previously collected data.

[32] The Joint Statement of Principles (February 2012) is available at www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

[33] Information on Kids' Privacy and COPPA is available at http://www.onguardonline.gov/articles/0031-kids-privacy; also see the FTC's December 2012 report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, at www.ftc.gov/opa/2012/12/kidsapp.shtm.

[34] According to leading mobile app analytics company Flurry, 24 percent of app revenues in 2011 came from mobile advertising, 24 percent from app sales, and 52 percent from in-app purchases, cited in the Association for Computing Technology's Apps across America, available at www.actonline.org/files/Apps-Across-America.pdf.

[35] Many of the recommendations in this section are drawn from Lookout Mobile Security's Mobile App Advertising Guidelines, available at www.lookout.com/resources/reports/mobile-ad-guidelines. GSMA's Privacy Design Guidelines for Mobile Application Development, available at www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development also provided valuable perspectives.

[36] See note 31 above.

[37] This statute is just one of the privacy laws and regulations that may apply to mobile applications and online services. For a listing of the major state and federal privacy laws, see the Privacy Laws page of the California Attorney General's web site, at www.oag.ca.gov/privacy.

California Department of Justice
Privacy Enforcement and Protection Unit

www.oag.ca.gov/privacy