Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps

Introduction

Canada's privacy laws require all businesses to balance innovation and entrepreneurialism with effective privacy protection. This applies to mobile app developers, whether they work on their own, or on behalf of an organization.

The mobile environment, along with the new app economy it has generated, is a rapidly evolving new frontier. As with past frontiers, it is filled with both richness and potential, but also risks. For example, while apps such as new reference tools and games are now part of our daily lives, there continue to be reports of unauthorized access to user information, including address books, photos and location data. Mindful of these developments, the Privacy Commissioners of Canada, Alberta and British Columbia have written this guidance document to help app developers in Canada to address the unique characteristics of the mobile environment which we believe create special challenges for protecting privacy.

The first challenge is that while the smart phone era brings unparalleled consumer connectivity and convenience, it also holds the potential for comprehensive surveillance of individuals. The novel uses of device sensors in apps, such as those that permit location awareness, provide the potential to follow where we go and, when combined with data on what we do and what we think, ultimately, to create a portrait of who we are.

Second, conveying meaningful information about privacy choices is not a simple exercise even in a desktop environment, and the challenge for app developers is compounded in the mobile space with a small screen and intermittent user attention. These design characteristics clearly add to the difficulty in reaching users with the right information about their privacy rights, in a form they could understand and at the right time for them to make informed choices.

A third challenge is the seeming lightning speed of the app development cycle and the potential to reach hundreds of thousands of users within a very short period of time. Given this rapidly evolving situation, Privacy Commissioners believe that it is important to proactively set out how those organizations that develop and launch mobile apps are required to meet their obligations under privacy laws and to support them in doing so.

It is important to recognize the complexity of the mobile app ecosystem and the many players who potentially can access personal information, including developers, service providers, app platforms, and advertisers. All stakeholders have a role to play in protecting the privacy of app users. This guidance is targeted to app developers: it focuses on the design and development of apps and the need to keep privacy top of mind in that creative process. In the future, we may address app privacy from other perspectives.

This guidance has been prepared jointly by the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioner of Alberta and British Columbia to draw your attention to key privacy considerations when designing and developing mobile apps. Additional sources can be found at the end of this document.

Make User Privacy Your Competitive Advantage

Whether you are the developer of a popular game that's available free of charge, or a health app that monitors a user's vital signs and is offered for a fee, it is ultimately in your interest to embrace privacy protection. In a 2012 survey of Canadian businesses, 39% viewed privacy as a competitive advantage, while 24% saw it as a significant advantage. They are right to do so: those mobile apps that take privacy seriously will be the ones that stand out from the crowd and gain user trust and loyalty. Significantly, a 2012 survey by the Pew Research Center revealed that 57% of app users in the United States have either uninstalled an app over concerns about having to share their personal information or declined to install an app in the first place for similar reasons.

Privacy can be a key competitive advantage for mobile app developers in Canada. A 2012 Canadian Wireless Telecommunications Association consumer study found that only 22% of smart phone users were receptive to the idea of providing an app developer with either demographic or location-based information about themselves, in order to receive an app for free. In the Office of the Privacy Commissioner of Canada's 2011 public opinion survey, almost two thirds of Canadians (65%) agree that protecting personal information will be one of the most important issues facing Canada in the next 10 years. And roughly nine out of 10 were concerned with businesses requesting too much personal information, not keeping information secure, and selling it to other organizations. These findings demonstrate that Canadians are concerned about privacy in the mobile space.

How does Privacy Law Apply to App Developers?

Under Canadian privacy laws, you are responsible for the personal information collected, used and disclosed through your app. At the federal level, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) sets ground rules for how organizations may collect, use or disclose information about individuals in the course of commercial activities. The law also gives individuals the right to see and ask for corrections to information an organization may have collected about them.

PIPEDA applies to organizations engaged in commercial activities across the country, except in Quebec, Alberta and British Columbia, which have their own private sector privacy laws similar to PIPEDA.[1]

While this guidance is intended for the private sector, developers who may also be building apps for governments, public bodies or health custodians should be aware of, and able to comply with, other privacy laws across Canada.

What is considered personal information?

No matter what kind of app you develop, your activities are likely subject to one of Canada's privacy laws because they may involve the collection, use and disclosure of personal information. The concept of personal information generally means information about an identifiable individual. Photographs and Internet Protocol (IP) addresses have been found to meet the definition in specific circumstances, and there are several other types of data collected by mobile apps that could be considered personal information.

For example, contact lists reveal details about the contacts themselves and also a user's social connections. Voice print biometrics, used for example in voice recognition apps, involve the collection of the characteristics that make an individual's voice unique. Location information can reveal user activity patterns and habits. Whatever method is used to link a device to its owner, whether it's a unique device identifier or multiple linked identifiers, it has the potential to combine with personal information to create a profoundly detailed and sensitive profile of a user's behaviour depending on the circumstances.

Combining disparate bits of information, derived from multiple sources, can also lead to detailed profiles that enable individuals to be identified. The Federal Court has ruled that information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

What about "commercial activity"?

Even if you aren't generating revenue from an app, you may still be covered by Canadian private sector privacy laws.[2] Collecting, using and disclosing personal information to improve user experience, which indirectly contributes to the commercial success of your app, could still be considered a commercial activity under the law.

Key Privacy Considerations For Developing Mobile Apps

The unique nature of personal information flowing through mobile devices, the challenge of the small screen, and the speed of the mobile app development cycle all make for a unique environment that underscores the need for comprehensive privacy protections. In the mobile environment, all of the different parties involved in handling users' personal information, including developers, service providers, app platforms and advertisers, are obligated to respect Canadian privacy laws. Developers, as creators of the apps, have a significant impact on users' privacy, either directly or through the company they work for.

1. You are accountable for your conduct and your code.

Under Canada's private sector privacy legislation, an organization is accountable for personal information that it collects, uses and discloses. Setting good practices for managing privacy doesn't need to be complicated or difficult. Anyone, from a one-person operation to a large company, can build a privacy management program. It starts with identifying someone within your company to be responsible for privacy protection, even if you only have a small team.

The process of developing a privacy policy will help you to inspect your own practices in a systematic way. When you are in the planning stages for an app, it's important to describe the data collection, usage and flows, along with the privacy and security policies under which the data is being both received and accessed. These descriptions need to be mapped and evaluated to ensure that they comply with your company's privacy policy.

Putting in place privacy rules for your business will help you manage risks in a timely manner, such as personal information leaking from your app. And given the potentially high number of users for your app, it will also help you to respond to requests for access to their personal information and complaints in an organized manner.

You should also ensure that all of your business arrangements and contracts are compliant with privacy laws because you are ultimately accountable. Make sure you have controls in place such as contracts to ensure that third parties process personal information in accordance with their obligations under privacy law, and make sure the controls are aligned with user expectations. You should be cautious when using third party code or software development kits — such as those from advertising networks or analytics providers – which could contain code you aren't aware of, such as aggressive adware or malware.

For additional guidance on accountability, consult *Getting Accountability Right with a Privacy Management Program*, which was prepared jointly by the Offices of the Information and Privacy Commissioners of British Columbia and Alberta, and the Office of the Privacy Commissioner of Canada.

2. Be open and transparent about your privacy practices.

Privacy laws require you to inform app users, in a clear and understandable way, what you are doing with their personal information. Transparency is also what users increasingly expect and transparent actors are rewarded with user trust and loyalty.

App development practices are drawing attention

Various data protection authorities, governments and consumer groups around the world are paying attention to how apps handle personal information. App developers are also responding to consumer demand for transparency, by providing guidance and launching apps that give the user a window into the data that is being collected, used and disclosed from their device by other apps. Several of these sources are listed at the end of this document.

Before users download your app

Users should not have to search for your app's privacy policy. They need clear and accessible information to evaluate what you are proposing to do with their information.

For example, wherever the app is being made available for download, tell potential users what personal information your app will be collecting and why, where it will be stored (on the device or elsewhere), who it will be shared with and why, how long you will keep it, and any other issues that will affect user privacy.

Once users have downloaded your app

You should have a monitoring program in place to make sure that the app in fact handles personal information in the way described in your privacy policy. And should you make updates to your app's privacy policy, inform users in advance and give them reasonable time to provide feedback before you implement changes. Tell users exactly what rules you are changing so they don't have to compare the new and old policies to understand what's happening.

If you are changing the app privacy policy to include new uses, especially transfers of information to third parties, make the changes easy to find and understand through the update process. *Never* make silent app updates that will diminish the user's privacy.

Specific notifications are needed

While your app's privacy policy tells the user about your practices, you should also provide specific, targeted notifications to users when they need to make a decision about whether to consent to the collection of their personal information. More detail on how to develop appropriate notifications is found under Sections 4 and 5 of this document, which focus on the timing of notices to users and obtaining consent on a small screen.

3. Collect and keep only what your app needs to function, and secure it.

Collect and keep only what you need

Consider whether you need to collect personal information at all. If you do collect it, privacy legislation requires you to limit the collection of personal information to what is needed to carry out legitimate purposes. It is possible to imagine instances where personal information could be used for extra features in an app beyond its core function. For example, an app for children that allows them to practice basic math functions could consider collecting the parents' email address in order to provide them with updates on their child's progress. But a child could just as easily complete addition and subtraction problems without providing any personal information.

If an app collects personal information, then privacy law requires you to justify why each piece of personal information is collected and how it is used by your app. Once you've done this you will be able to tell users what your app does with their personal information, why it does it, and what their choices are. Using the math app example, this means allowing parents to opt out of providing their email address if they do not wish to track their children's progress.

If you cannot explain how a piece of information is related to the functioning of your app, then you probably should not be collecting it. For example, it is not clear why a time management app would need to collect a user's location or their date of birth.

While it may be tempting, you should avoid collecting data because you believe it may be useful in the future. Canadian privacy laws require you to restrict your data collection to what is needed for an identified purpose that exists now and delete data that you no longer need for the original purpose for which it was collected.

A key feature of privacy protection, with respect to non-sensitive information, is allowing users to opt out of data collection.[3] So, if you are sharing behavioural information or device identifiers with third parties (such as an ad network), your privacy policy should identify those third parties and link to information about how to modify or delete the data. You should also provide a means for users to opt out of such tracking.

Apps should be designed in a way that does not require you to collect any device-unique identifiers if it is not essential to the functioning of the app. Avoid associating data across apps unless it is obvious to the user and necessary to do so. If you must make links, ensure that sensitive data is not linked to a user's identifier for longer than it needs to be.

For example, if your app transmits personal information, you should not log it unless it is necessary. If you have to log it, secure it and delete it as soon as possible.

Avoid collecting information about a user's movements and activities through the use of location and movement sensors unless it relates directly to the app and you have the user's informed consent. Never collect sound or activate the device camera without the specific permission of the user.

Similarly, avoid collecting personal information about third parties from a user's device unless you have consent.

Make sure you secure what you collect

You should have the appropriate controls in place both on the mobile device and on the backend systems that will store the information to ensure the security of the personal information being handled. Security safeguards should be appropriate to the sensitivity of the information. Users' information should be encrypted when it is stored and when it is transmitted over the Internet.

Ensure that users have a clear and easy way to refuse an update, deactivate and delete the app. You should give users the ability to delete all of the data collected about them. In particular, when users delete an app, their data should also be deleted automatically.

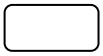
To help evaluate your personal information protection readiness, you can consult the *Securing Personal Information: A Self-Assessment Tool for Organizations*, which was prepared jointly by the Offices of the Information and Privacy Commissioners of British Columbia and Alberta, and the Office of the Privacy Commissioner of Canada.

4. Obtaining meaningful consent despite the small screen challenge.

There's been no shortage of discussion on the need to improve privacy rules and settings on the small screen of a mobile device. The challenge is to show users, in a creative and meaningful way, what is actually happening with their personal information. After all, no one wants to read a 20 page privacy policy on a small screen.

As a result, consider the right information strategy for the job of reaching app users without causing "notice fatigue," where people ignore notices or warnings they see too often. You can also benefit from work others have done in this area for meaningfully conveying privacy rules on small screens. Some organizations are offering mobile privacy policy template language and generators, but you need to assess whether the results they provide meet not only your objectives, but also your obligations under Canada's privacy laws. Here are some options for visual cues that may be helpful:

Layering the information: Put important details up front in your privacy policy but embed links to the details of your privacy rules so that those who want more detail can find it. Make sure that the top layer draws users' attention particularly to any collection, use or disclosure of information that they would not otherwise reasonably expect.



Providing a privacy dashboard: It may also be beneficial to display the user's privacy settings with a tool that allows users to tighten their settings. Approach this display in a way that encourages user action, such as with the use of radio buttons rather than web links. As well, instead of just using an on/off button, explain to users the consequences of making a choice to provide data so they can make an informed decision. Also, ensure that users have a way to modify their information, opt out of any tracking and delete their profile entirely if they wish.

Rather than just using text, you can make a more impactful privacy policy by using the following:

Graphics: The first layer of your mobile privacy policy could primarily be icons, labels or images, as long they are linked to text that provides more detail. You could also make use of graphics in the app at the moment when sensitive information is about to be transmitted and user consent is required. For example, if your app is about to access the user's location data, you could activate a symbol to raise user awareness of what is happening and the reason for it, as well as the user's choices.

Colour: Drawing the user's attention by using colour and altering its intensity may be a way to alert the user. The intensity of the colour could be scaled to the importance of the decision or sensitivity of the information.

Sound: Selective use of sounds and scaling the device's volume, to alert the user may be another appropriate way to draw attention to a privacy-related decision that needs to be made in a timely way.

5. Timing of user notice and consent is critical.

Communicating with users about privacy in the mobile app environment is complicated by the fact that user attention in this space is intermittent and limited. This makes it important to be thoughtful and creative when deciding at which points during the user's experience privacy messages will have the most impact.

It is important to inform users about your app's privacy practices when the users download the app and to obtain their consent. However, more is needed. Users cannot be expected to remember months later information they read when downloading an app, especially given that they may have many apps on one mobile device. This limits the value of obtaining one-time user consent. Privacy messaging carries more weight if it is delivered at the right time.

In other words, tell users in advance what will happen with their information with the eventual use or deployment of the app and also in real time, while it's actually happening. With this design challenge in mind, it's crucial that the users are able to make timely and meaningful choices. For example, if your app is about to actively access the user's location data, you could activate a symbol to raise user awareness of what is happening. If your app takes photos or video, make sure to clearly state whether your app will tag the images with location data and allow the user to opt out of this feature at the time of taking the photo or video.

Privacy practices should be highlighted during the purchase process but also upon first use of the app. Depending on the purpose of your app, you may wish to give users control over repeated prompting to avoid notice fatigue, but the user should be able to set a period of time after which the consent should be renewed.

Conclusion

In Canada, there is an expectation and a legal requirement that app users are to be informed of what information is being collected, used and disclosed about them, as a matter of transparency and openness, and for their consent to be meaningful. Given the popularity of apps, you can expect increased scrutiny of the privacy practices in your industry in the years ahead – both by regulators and the market itself, driven by increasingly informed, discerning and influential consumers.

This guidance has been prepared to help you improve your privacy practices and the features of your app, as both are fundamental to helping users decide which apps they will trust and continue to use. Following these good practices will help to reassure users that you have given the protection of their privacy the attention it deserves.

Checklist: Key Privacy Considerations For Developing Mobile Apps

You are accountable for your conduct and your code.

- Your company, which may just be you, is responsible for all personal information collected, used and disclosed by your mobile app.
- Make sure to have controls in place, such as contracts or user agreements, to ensure that third parties accessing personal information through your app are respecting their privacy obligations.
- Map out where the information is going and identify potential privacy risks.

Be open and transparent about your privacy practices.

- Develop a privacy policy that informs users, in simple language, what your app is doing with their personal information.
- Post a privacy policy where users can easily find it, and where it is readily accessible to potential users who are considering downloading your app.
- Have a monitoring program in place to ensure that personal information is being handled in the way described in your privacy policy.
- When updating an app, inform users of any changes to the way their personal information is handled, and give them an easy way of refusing the update.

Collect and keep only what your app needs to function, and secure it.

- Limit data collection to what is needed to carry out legitimate purposes.
- Do not collect data because you think it may be useful in the future.
- Allow users to opt out of data collection outside of what they would reasonably expect is necessary for the functioning of the app.
- Have the appropriate safeguards in place to protect the personal information you are handling. Use encryption when storing and transmitting data.
- Give users the ability to delete the personal information your app has collected. If they delete the app, their data should be deleted automatically.

Obtaining meaningful consent despite the small screen challenge.

- Select the right strategy to convey privacy rules in a way that is meaningful on the small screen. This could include:

    - o layering privacy information, placing important points up front and providing links to more detailed explanations; and
    - o A privacy dashboard that displays a user's privacy settings and provides a convenient means of changing them.
    - o Visual cues such as graphics, colour and sound to draw user attention to what is happening with their personal information, the reasons for it, and choices available to the user.

Timing of user notice and consent is critical.

- Users should be told how their personal information is being handled at the time they download the app, when they first use the app, and throughout their app experience, to ensure that their consent remains meaningful and relevant.
- Be thoughtful and creative when deciding when to deliver privacy messages to most effectively capture users' attention and achieve the most impact at the right time, without causing notice fatigue. For example, if your app is about to actively tag photos with the user's location data, you could activate a symbol as a cue to the user, providing them with a choice to refuse.

Sources:

Privacy Oversight Offices involved in writing this document

Office of the Privacy Commissioner of Canada
Information and Privacy Commissioner of Alberta
Information and Privacy Commissioner for British Columbia

Implementing Privacy Rules for Your Business

Privacy laws and oversight offices in Canada
Getting Accountability Right with a Privacy Management Program and *Securing Personal Information: A Self-Assessment Tool for Organizations* are joint publications of The Office of the Privacy Commissioner of Canada, and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia.
The Office of the Privacy Commissioner of Canada has developed a number of tools that will be of use to organizations to learn the basics about privacy and privacy legislation. These include: *Your Privacy Responsibilities: A Guide for Businesses and Organizations*; *Privacy Questionnaire: Is Your Business Ready*? and a video for small- and medium-sized organizations entitled *PIPEDA for Business: What you need to know about protecting your customers' privacy*.
The Information and Privacy Commissioner of Alberta has developed the following documents which will be of assistance: *Guide for Businesses and Organizations on the Personal Information Protection Act*; *Information Privacy Rights*; and *10 Steps to Implement PIPA*.
The Information and Privacy Commissioner of British Columbia has also developed similar tools relating to BC's private sector legislation including: *What are My Organization's Responsibilities Under PIPA?* and *A Guide for Business and Organizations to BC's Personal Information Protection Act*.

Selected Privacy-related Guidance for App Developers

Berkeley Center for Law & Technology, *Mobile Phones and Privacy*, July 10, 2012
Calo, M. Ryan. Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame Law Review 1027 (2012)
California Auditor General and mobile application platforms' joint statement on privacy, February 2012
Electronic Frontier Foundation, Mobile User Privacy Bill of Rights, March 2, 2012
Future of Privacy Forum and the Center for Democracy & Technology, Best Practices for Mobile Applications Developers (July 2012) and the Future of Privacy Forum's site for app developers
GMSA, Mobile and Privacy: Privacy Design Guidelines for Mobile Application Development, February 2012
Happtique Draft App Certification Program, July 2012
Lookout Mobile App Advertising Guidelines June 2012
OASIS Privacy Reference Management Model Version 1.0 Committee Specification Draft, March 26 2012
Pew Research Centre, Privacy and Data Management on Mobile Devices, September 2012
PrivacyChoice Mobile Resources
TRUSTe Mobile Privacy Solutions

United States Federal Trade Commission, Marketing Your Mobile App: Get It Right from the Start, August 2012
United States Federal Trade Commission Staff Report, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing, February 2012
United States National Telecommunications and Information Administration, Privacy Multistakeholder Process: Mobile Application Transparency, August 2012

Communicating Privacy Rules on Small Screens

Know Privacy policy coding methodology
Privacy Icons (beta)

Selected Mobile App Privacy Rating Tools

Clueful
LBE Privacy Guard
Lookout Premium
MobileScope

---

[1] New Brunswick and Ontario also have laws substantially similar to PIPEDA with respect to health information custodians (October 4, 2012).

[2] Please see the definition of "organization" in Alberta's and British Columbia's legislation.

[3] See the Framework for Opt-Out as explained in the Office of the Privacy Commissioner of Canada's Policy Position on Online Behavioural Advertising (July 2012).