Improving Privacy Practices for Legal Apps: A Best Practices Guide

March 2019

Authored by: Amy Salyzyn
Teresa Scassa
Jena McGill
Suzanne Bouclin

Acknowledgements

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

Over the course of the preparation of this document we sought and received comments and input from a number of stakeholders in the legal technology community, including developers and lawyers. We are very grateful for all comments and feedback we received. They were very helpful in improving our final document. All errors or omissions are, of course, our own.

We are also thankful for the assistance that we received from several research assistants at the University of Ottawa throughout the course of this project, including Pam Dheri, Lora Hamilton, Nathan Hoo, Nicolas Karsenti, and Salman Rana.

Purpose of this Best Practices Guide

This Best Practices Guide aims to help developers and providers of legal applications ("apps") design and share apps that adopt best privacy practices.

This Guide focuses on the ten Fair Information Principles in the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). While not exhaustive of an organization's obligations under PIPEDA, the Fair Information Principles address important privacy-related topics such as:

- Defining "personal information";
- Providing adequate notice to users about collection, use and disclosure of personal information;
- Obtaining consent; and
- Data security.

A full list of these principles can be found here.

PIPEDA does not apply to all legal apps. Later in this Guide, we describe when PIPEDA might apply to a legal app.

If PIPEDA *does* apply to the app that you are developing or providing to the public, this Guide will help you understand what you need to do to comply with this legislation. However, even if PIPEDA *does not* apply in your case, this Guide will still be useful to you: adopting good privacy practices can attract users and reduce exposure to the negative reputational and monetary consequences associated with privacy breaches. Additionally, even if PIPEDA does not apply to your app for jurisdictional reasons, there may be substantially similar provincial privacy laws that apply and this Guide may be useful in helping you comply with these laws.

Please Note:

This Guide was completed in March 2019. As time passes, changes to the relevant legal and technical environments may impact what constitutes a best practice on a particular privacy issue.

This document is not intended to provide legal advice. The guidance provided should not be understood or treated as legal advice. If legal advice is required, users should consult a lawyer.

What is a Legal App?

There is no single definition of a "legal app". This Guide adopts a flexible definition which includes **mobile** and **web-based resources** that purport to assist individuals with **legal tasks**.

Examples of Legal Apps

There are several different types of legal apps available to the public in Canada, and many more are likely to be developed over time. Some legal apps are designed to walk self-represented individuals through court or tribunal processes; some are designed to assist individuals in preparing legal forms; some assist individuals in finding lawyers; and others provide rapid access to legal information or even help users collect evidence.

Format of this Guide

This guide is presented as a series of questions and answers, followed by a "Developer Checklist."

PRIVACY QUESTIONS AND ANSWERS FOR LEGAL APPS

1. Will PIPEDA apply to my legal app?

Brief Answer:

If there is a commercial dimension to your legal app (such as monetization through a fee for download, advertising or selling data), PIPEDA will very likely apply.

Note that PIPEDA does not apply if the commercial activity at issue takes place solely in Alberta, British Columbia or Quebec. However, these three provinces have privacy legislation that is substantially similar to PIPEDA. It should also be noted that PIPEDA applies to commercial activities that cross provincial or national borders.

PIPEDA applies to any organization that collects, uses, or discloses personal information in the course of commercial activity.

In determining if PIPEDA applies to your legal app, the key words in this definition are "organization", "personal information" and "commercial activity". All of these terms are interpreted broadly in the legislation.

If you are providing a legal app to the public, you are likely to be considered an **"organization."** The term includes individuals, corporations and non-profit organizations. There are some narrow exceptions, such as if your organization collects, uses or discloses personal information for only journalistic, artistic or literary purposes.

"Personal information" includes any information that raises "a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information" (OPC Interpretation Bulletin, "Personal Information"). Such "personal information" could be: a user's name and contact details, financial or payment information, log-in information, or location information. It can also include the fact that a user accessed the app, a user's contact lists (which will contain the personal information of the contacts), click stream data, IP addresses, device identifiers, and search queries. If your app communicates with users over the internet or via mobile technologies, there is a very strong chance that your app collects, uses or discloses personal information.

"Commercial activity" refers to more than just providing information by way of an app for which a fee is charged (although this would certainly be commercial activity). Commercial activity also includes apps that are free to download but include:

- in-app upgrades for a fee ("freemium");
- access to content on a subscription basis;
- in-app purchase options;
- banner or pop-up advertising;
- payment by third parties for referrals (e.g. a legal app refers a user to a lawyer and the lawyer pays a fee to the app providers);
- promotion for the services of the law firm/company that provides the app (through advertisements, or through "credits" towards legal advice); and
- monetization of user data whether identifiable or de-identified.

Example: App Co. is based in Alberta. It provides a free app that allows users to estimate the cost of legal services for certain matters based on user responses to a series of questions. One of the variables is the province in which the matter will be dealt with. Although the app is free, App Co. sells aggregate data based on the answers to its questions. PIPEDA applies to App Co.: App Co. is engaged in commercial activity, and although based in Alberta (where there is a substantially similar provincial law), its activities are not confined to that province and cross provincial boundaries.

PIPEDA applies to commercial activities within all Canadian provinces or territories except for Alberta, British Columbia and Quebec. It should be noted, however, that these three provinces have privacy legislation that is substantially similar to PIPEDA and this Guide may be useful in helping you comply with these laws.

It should also be noted that PIPEDA applies to commercial activities that cross provincial or national borders.

2. What makes legal apps different from other apps for privacy purposes?

Brief Answer:

Legal apps raise unique privacy concerns such as: (1) user confusion as to whether solicitor-client privilege or lawyer confidentiality applies; (2) the collection of especially sensitive information relating to legal problems experienced by the user; (3) heightened interest on the part of third parties (such as law enforcement or adverse parties in a lawsuit) in requesting or compelling the disclosure of the personal information collected; and (4) special concerns arising where the app engages with court data or a public registry.

Helpful guidance documents tailored to offering best privacy practices when it comes to apps generally already exist. The federal Office of the Privacy Commissioner (OPC), for example, has published some guidance here. This Guide aims to supplement this and other general guidance by speaking specifically to the context of *legal* apps. What unique privacy concerns might arise in the context of legal apps?

One concern is that a user may mistakenly believe that, by engaging with a legal app, they are entering into a situation where solicitor-client privilege or lawyer confidentiality applies. **If your app does not create a lawyer-client relationship or otherwise facilitate communications between a lawyer and his or her client**, you should make it very clear to users that the information that they are sharing does not receive any special protections and could potentially be used against them in a legal proceeding.

Example: Mary experiences non-consensual sexual contact on a date. She does not immediately report to the police. Instead, Mary decides to consult a lawyer. She uses an app designed to connect individuals with lawyers who have expertise appropriate to the legal concern at issue. The app uses textual analysis, so users are asked to type in up to 100 words describing their problem. Mary types in: "I am not sure if I was raped and I don't know if I should go to the police or if I should sue." Because no solicitor-client relationship is in place, Mary's statement (which expresses uncertainty about what happened) could be obtained under a court order by defence counsel in either criminal or civil proceedings, if it is recorded or stored by the app.

Another way in which legal apps may be different from many other apps is that **the information they collect may be uniquely sensitive**. This is particularly the case if the app is being used to obtain information about a legal problem faced by the user of the app. For example, the simple fact that a user is consulting a legal app about initiating divorce proceedings or obtaining a criminal pardon (for example) may be sensitive personal information. Apps that help users collect evidence – like, for example, apps that are designed to assist users in filming encounters with the police – are also likely to be gathering sensitive information. The sensitivity of the information that is collected, used, or disclosed has an impact on **consent**, on the measures needed to ensure **data security**, and on the threshold for **data security breach notification.** The details of this impact are discussed below in Question 7.

In the legal app context, the potential lack of privilege and the potential sensitivity of the personal information collected can pose heightened risks because of **the possible interest of third parties in requesting or compelling the disclosure of this information.** For example, "police encounter" apps may generate particular vulnerabilities for users. Specifically, while these apps inform individuals of their rights during interactions with police, they may also offer audio and video-recording functions, which can generate content of interest to legal authorities. Similarly, apps that assist individuals in resolving legal disputes outside of court may collect information – including financial information – that is discoverable to an opposing party if the matter proceeds to civil litigation.

Finally, **if a legal app engages with court data or a public registry**, care must be taken to only collect or disclose the personal information contained in those published data or documents for a purpose directly linked to why the information was made publicly available by the court or registry. Question 6 addresses this issue in more detail.

3. What is Privacy by Design and what does it mean for legal apps?

Brief Answer:

Privacy by Design emphasizes and prioritizes privacy principles throughout the design stage of a project or a service. The proactive nature of this approach can reduce user exposure to privacy risks. Implementing a Privacy by Design approach could include, for example, choosing from the outset of the development process to limit the collection of personal information from users, either by collecting less information or by de-identifying data.

Privacy by Design emphasizes and prioritizes privacy principles throughout the design stage of a product or service. Privacy by Design is considered a best practice insofar as it can help to reduce user exposure to privacy risks and breaches.

There are many design choices that can support privacy. Perhaps most obviously, you can **limit the collection** of personal information (**limiting the collection** of personal information is

required for PIPEDA compliance and is important in minimizing the risk to users in the event of **data security breaches**). In some cases – such as where an app developer or provider wishes to collect certain data to sell or to recover costs of developing and updating the app, or for research purposes – it is important to consider how much of that information must actually be linked to identifiable individuals. For example, anonymized or aggregate data may be all that is required for commercial or research purposes, and de-identification at the point of collection may be the most protective privacy measure that still permits meaningful data to be collected, used and disclosed for other purposes. Data that cannot be linked to an identifiable individual is not "personal information" for the purposes of PIPEDA and therefore the legislation does not apply to it. However, not every de-identification process will sufficiently anonymize personal data, leaving it capable of re-identification. In such cases, the de-identified data may still be considered personal information and consequently will be subject to PIPEDA. According to the OPC, information is personal information if there is a "serious possibility" that a person could be identified through the use of that information, alone or in combination with other information from any source.

In a now classic example of re-identification risk, AOL chose, in 2006, to publish de-identified data about its users' search queries. Two journalists who combed through the data were successfully able to identify a woman. Also in 2007, two researchers quickly linked de-identified customer data published by Netflix to specific individuals.

For many legal apps that are developed in non-commercial contexts (for example, in law school courses or by non-profit organizations) PIPEDA may not apply at the outset or in their beta stages. However, this is not a reason to ignore privacy at the design stage. A developer who creates an app in a non-profit context and later seeks to commercialize it will want to have an app that has been designed with privacy in mind and that is compliant with the law. Even if PIPEDA does not ultimately apply to a particular legal app, users stand to benefit regardless when a developer chooses to enhance transparency and better protect personal information.

4. What do I need to consider if I build my app on a pre-existing platform or if I use third-party code?

Brief Answer:

Using pre-existing platforms or third-party code to build apps may result in unexpected privacy risks. One significant issue is the potential for third-party collection and use of personal information. Developers need to be sure they understand if and how any third parties are gathering and using the personal information collected via their apps and should take the necessary steps to ensure compliance with PIPEDA (like, for example, ensuring appropriate notice is given to users and consent is obtained).

Developers who want to minimize start-up costs or otherwise take advantage of pre-existing efficiencies may look for tools or resources that assist them in building and disseminating their products. These tools and resources may give rise to specific privacy concerns and risks, some of which are discussed below.

For example, some companies assist developers by offering a platform through which apps can be developed and which provides certain back-end functionalities. Developers should be aware that these platforms may collect personal information from their users. They should read and understand the privacy policies of these platforms and should consider whether the policies pose privacy risks for their actual or targeted users. Developers relying on third party platforms may be required by PIPEDA to provide notice to users of their app that personal information may be collected by a third-party when the app is used.

Privacy risks can also arise from using third-party code to deal with discrete functions when developing an app. In a recent study, researchers considered the use of "libraries" by app developers (i.e. third-party "software code that deals with a particular task or function") and observed that privacy issues arise "when these libraries send information off the device to a third party and the third party then collects and uses that information."[1] The researchers gave as examples the use of analytics libraries and ad libraries.

In the study, the researchers observed, among other things, that where apps used third-party code, there was often a discrepancy between how the app's privacy policy described how personal information would be used and how the personal information was *in fact* being used. Where such a discrepancy exists, there are obvious privacy issues: appropriate notice has likely not been given to users regarding how their information will be used and appropriate consent has likely not been obtained in relation for the use of the information (the issues of notice and consent are discussed in more detail below).

Moreover, the researchers noted that the ways in which libraries may be using and collecting information can generate additional concerns. For example, developers who install ad libraries from ad networks may be creating unintended privacy issues for their users:

> Because so many apps are monetized through advertising and may be communicating with the same ad networks, information like device ID also allows ad networks to track individual user behaviour across multiple apps. Depending on what information ad networks have in relation to individuals, they might also be able to track user behaviour across devices. This is why users might have the experience of looking at an item while browsing on their computer and then seeing an ad for something similar delivered to them from within a mobile app on their phone. In addition, some ad networks are run by companies like Facebook and Google, which have access to a wealth of data from multiple activities for profiling purposes.[2]

---

[1] Austin, Lisa M. and Lie, David and Sun, Peter and Spillette, Robin and D'Angelo, Mariana and Wong, Michelle, Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project (June 27, 2018). Available at SSRN: https://ssrn.com/abstract=3203601 or http://dx.doi.org/10.2139/ssrn.3203601.

[2] *Ibid* at 25.

Legal app developers who are using ad libraries should consult the OPC's guidance on behavioural/targeted advertising.

5. Are there limits to what personal information I can collect, and if so, what are they?

Brief Answer:

Personal information can only be collected for purposes that "a reasonable person would consider are appropriate in the circumstances". Moreover, the amount and nature of the personal information collected must be necessary to achieve the purposes for which the information is collected.

Under PIPEDA, a legal app can only collect personal information that is **necessary** to achieve the purposes for which the information is collected. Additionally, personal information can only be collected for purposes that **"a reasonable person would consider are appropriate in the circumstances."**

Example: XYZ Labs has developed an app that allows individuals to obtain information on filing for bankruptcy. A company that provides bankruptcy-related services would like to know whether and where there are concentrations of demand for the kinds of services they provide. They would like to purchase location information relating to users of XYZ's app. If XYZ decides it would like to collect location information from app users' phones in order to build a revenue stream, it must notify its users that location data will be collected, and it must obtain consent to its use and sharing. Collection of location data can be by default (so long as there is notice and consent), or it can be done only where users specifically opt in to the collection. Opt-in is a more privacy-friendly approach.

Before collecting any personal information, you must clearly identify to the user the purposes for which you are collecting this information.

You will want to consider how to structure default settings in a way that enables users to easily make informed decisions about protecting their personal information. The issue of consent is dealt with in further detail in the answers to Questions 6 and 7.

6. Do I need consent from users to collect, use or disclose their personal information?

Brief Answer:

As a general rule, the knowledge and consent of the user are required for the collection, use and disclosure of personal information. Exceptions to this general rule that may be particularly relevant in the context of legal apps include the collection, use or disclosure of publicly available personal information, and the requirement to disclose personal information to comply with a subpoena, warrant or rules of court relating to the production of records.

Collection: For legal app developers, there will be very few exceptions to the requirement of consent to collection. If your app collects **personal information** from users (as discussed above under "personal information") you will need to obtain **consent**. (See the answer to Question 7 for details on how consent is to be obtained).

One exception to the consent requirement for collection of personal information that may be relevant to legal app developers is the exception for **publicly available personal information**. This exception applies to, among other things, information contained in public registries or court and tribunal records. For this reason, the exception may be of particular interest to legal app developers. For example, a legal app that helps users find relevant cases or tribunal decisions will not need to obtain the consent of the individuals whose personal information is featured in those documents. Similarly, a legal app that assists users in finding information in a public registry will not require the consent of the individuals whose names and personal information are found in the registry.

It is important to note that the exceptions to consent for publicly available personal information are only applicable where the collection of information is for a purpose directly linked to why the information was published in the court/tribunal decision, or registry. The Supreme Court of Canada has found that in the case of court and tribunal documents, the purpose of their online posting is to serve the open courts principle, which includes the goals of promoting "a shared sense that our courts operate with integrity and dispense justice" and providing "an ongoing opportunity for the community to learn how the justice system operates and how the law being applied daily in the courts affects them." Any use of personal information from court and tribunal records that does not serve these purposes or that serves other purposes as well will not fall within the scope of the exception to consent for publicly available information.

Use: Any "use" of personal information must be one "that a reasonable person would consider appropriate in the circumstances" (PIPEDA, s. 3). A "use" of personal information relates to the use made by the organization that has collected it. For example, an app developer might use an app user's email address to notify them of updates available for the app.

Disclosure: Generally speaking, consent is required for the disclosure of personal information to anyone outside of the organization that has collected it. For example, if you plan to share certain personal information about users with a third party, you must notify your users, explain the purpose of the sharing, and seek their consent.

There are circumstances in which information can be disclosed without a person's knowledge or consent. Some of the most important exceptions in the context of legal apps may be where disclosure is required "to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records" (PIPEDA, s. 7(3)(c)). For example, if an app collects video recordings of users' interactions with police, a police investigation may lead to a judge issuing a court order requiring disclosure of the video. If your app collects information that could be relevant to potential criminal or civil legal proceedings, you should make it clear to your users, in your privacy policy, that disclosure of personal information can be compelled by a court and that where this occurs you will be required to provide it.

Section 7(3) of PIPEDA contains an extensive list of exceptions to the knowledge and consent requirements. A recommended best practice is to consult the statute and obtain legal advice should questions arise about whether disclosure without the knowledge or consent of a user is permitted in a given situation. Moreover, if your app does, in fact, facilitate communications between a lawyer and his or her client, the potential impact of solicitor-client privilege on the ability to disclose pursuant to these statutory exceptions must also be considered.

7. How should I obtain consent for the collection, use or disclosure of personal information through my legal app?

Brief Answer:

The appropriate form of consent and the manner of seeking consent will vary depending on the circumstances. In general, express consent should be obtained where the information at issue is sensitive. Additionally, express consent should be obtained where the collection, use or disclosure of information is outside the reasonable expectations of individuals or creates a meaningful residual risk of significant harm. The OPC has released guidelines for obtaining meaningful consent, to which you should refer.

What constitutes meaningful consent under PIPEDA varies depending on the context and the type of information at issue. In guidance published in May 2018, the OPC advised that organizations must generally obtain **express consent** when:

- *The information being collected, used or disclosed is sensitive;*
- *The collection, use or disclosure is outside of the reasonable expectations of the individual; and/or,*
- *The collection, use or disclosure creates a meaningful residual risk of significant harm.*

There is no hard and fast definition of what constitutes sensitive information, and whether information is sensitive or not depends upon the context and circumstances. However, some information is presumptively sensitive.

For example, personal health information or personal financial information is generally considered sensitive. Information about a person's legal affairs or legal concerns may also be sensitive. Accordingly, if a legal app user is seeking information for help with a particular legal problem – like, for example, a bankruptcy, a criminal matter or a divorce – the mere fact that an identifiable individual has used the app could constitute sensitive personal information.

The OPC advised in its May 2018 guidance that to obtain meaningful consent and meet their related privacy law obligations, organizations must:

- *Make privacy information readily available in complete form: (1) What personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to; (2) With which parties personal information is being shared; (3) For what purposes personal information is being collected, used or disclosed, while giving emphasis or bringing attention to four key elements, in sufficient detail for individuals to meaningfully understand what they are consenting to; and (4) Risks of harm and other consequences;*
- *Provide information in manageable and easily-accessible ways;*
- *Make available to individuals a clear and easily accessible choice for any collection, use or disclosure that is not necessary to provide the product or service;*
- *Consider the perspective of your consumers, to ensure consent processes are user-friendly and generally understandable;*
- *Obtain consent when making significant changes to privacy practices, including use of data for new purposes or disclosures to new third parties;*
- *Only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate, under the circumstances;*
- *Allow individuals to withdraw consent (subject to legal or contractual restrictions).*

Example: The DebtHelp app allows users to search for answers to common legal questions about how to file for bankruptcy in Canada. The app works by having a user type in his or her own questions. It then shows the first two lines of possibly relevant answers with a notification that the full answer is available for a fee. The providers of the DebtHelp app have observed that many users do not purchase an answer on their first visit to the website. To encourage users to revisit the website and possibly purchase an answer in the future, the DebtHelp app wants to make use of re-targeting services that display advertisements about the DebtHelp app when these previous visitors are browsing the internet. Because re-targeting may inadvertently disclose sensitive personal information to third parties (i.e. those who have not visited the website themselves but who share a computer with someone who has visited the website), DebtHelp should consider whether it is possible to use re-targeting and still appropriately protect a user's personal information and, if so, whether they have obtained effective consent from users for this practice. The OPC's guidance on online behavioural advertising provides useful guidance.

8. Do I need to provide a privacy policy?

Brief Answer:

There is no express requirement that a legal app include a privacy policy. However, a privacy policy can be an efficient way to comply with PIPEDA requirements to provide information to users, as it allows you to put all of the relevant (and required) information in one place.

For example, if you are collecting, using or disclosing personal information in the course of commercial activity via a legal app, you are required to provide notice and other information to the users of your app, and to obtain their consent. PIPEDA also requires organizations to be transparent about their privacy practices.

In addition to a privacy policy, technological tools—like pop-up windows and privacy dashboards—can be used to provide timely notice to users about the collection of information, or other privacy related matters.

If you are collecting, using or disclosing personal information in the course of commercial activity via a legal app (see Question 1, above), you are required to provide notice and other information to the users of your app, and to obtain their consent. PIPEDA also requires organizations to be transparent about their privacy practices.

One way to do this is through a privacy policy, which allows you to put all of the relevant (and required) information in one place. A privacy policy typically sets out what personal information is being collected by the app and for what purposes. A privacy policy also provides information about with whom (if anyone) the information is shared, how it will be stored, how long it will be retained, and how it will be disposed of when it is no longer required. Additional information may include a contact person should users require additional information or wish to make a complaint.

The OPC offers guidance on how to prepare better online privacy policies that includes advice to "avoid templates and boiler-plate language"; use plain language, and advise users what choices they may have about how their personal information is dealt with.

In addition to a privacy policy, you can also use technological tools to provide timely notice to users about the collection of information, or other privacy related matters. For example, a pop-up window in your app could periodically remind a user that they have enabled the collection of certain personal information, and could provide them with an opportunity to turn off that feature, if they so choose. In the case of mobile apps, the OPC has provided the following suggestions for "obtaining meaningful consent despite the small screen challenge":

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.*

9. How long can I keep the personal information I have collected through my app?

Brief Answer:

Personal information should only be kept as long as it is necessary to fulfill the stated purpose.

Personal information should only be kept as long as it is necessary to fulfill the stated purpose. If, for example, you collect a user's email address in order to provide them with notifications about updates to your app, then as long as they remain a user of the app, it is appropriate to retain this information.

You should consider whether a user's account and account information will be retained indefinitely, or will be deleted if the app is inactive for a certain period of time (e.g., if it has not been used for a year). If an app is used for a specific activity, such as assisting the user in applying for permanent residency, or in applying for a legal pardon, it may not be necessary to retain the personal information collected once the process is completed. You might also consider providing users with the option to delete their accounts.

10. What is data localization and does it matter for legal apps?

Brief Answer:

Data localization refers to the storage of personal information within the jurisdiction in which it is collected.

PIPEDA does not prohibit the transferring of personal data to a third party organization that is located in another jurisdiction. There are, however, rules governing such transfers. In particular, it should be noted that you will remain accountable for the information which is in the hands of a third party and you are obligated to protect this information (this is typically done by way of a contract). If an app transfers personal information to third parties, it is also necessary to be transparent to users about this practice.

In some circumstances, developers and providers of legal apps may want to avoid transferring personal data to third parties outside of the country, even if such a transfer is legally permissible, due to concerns about potential disclosure to foreign law enforcement or national security agencies. These concerns are likely to be particularly important in relation to legal apps that engage with criminal law or immigration law issues.

Data localization refers to the storage of personal information within the jurisdiction in which it is collected. Data localization is meant to address concerns that personal information that crosses borders into other countries will be subject to the laws of those countries. Data localization is not required by PIPEDA. Under PIPEDA, information can be transferred to third party companies for processing, even if those companies are located in other countries.

There may be circumstances in which a legal app provider wishes to provide data localization. For example, users of a legal app that assists individuals in complying with new laws on the legal use, sale and cultivation of cannabis – which is legal in Canada but remains illegal throughout most of the United States – may wish to have information regarding their use of the app stored in a way that makes it inaccessible to U.S. law enforcement or national security officials.

The OPC has published guidelines on the issue of processing personal data across borders. The key findings in these guidelines are as follows:

- *PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing;*
- *PIPEDA does establish rules governing transfers for processing;*
- *A transfer for processing is a "use" of the information; it is not a disclosure. Assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required;*
- *The transferring organization is accountable for the information in the hands of the organization to which it has been transferred;*
- *Organizations must protect the personal information in the hands of processors. The primary means by which this is accomplished is through contract;*
- *No contract can override the criminal, national security or any other laws of the country to which the information has been transferred;*
- *It is important for organizations to assess the risks that could jeopardize the integrity, security and confidentiality of customer personal information when it is transferred to third-party service providers operating outside of Canada;*
- *Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities.*

In its guidelines on this issue, the OPC has also advised that, in some circumstances, transferring personal data to third parties outside of the country may be "unwise":

> *In the case of outsourcing to another jurisdiction, PIPEDA does not require a measure by measure comparison by organizations of foreign laws with Canadian laws. But it does require organizations to take into consideration all of the elements surrounding the transaction. The result may well be that some transfers are unwise because of the uncertain nature of the foreign regime or that in some cases information is so sensitive that it should not be sent to any foreign jurisdiction.*

This advice may be particularly salient in the case of legal apps that collect information related to criminal law or immigration law issues, and where disclosure of that information to foreign law enforcement or national security agencies may have serious consequences for some users.

11. What are my data security obligations for personal information collected by my legal app?

Brief Answer:

There are no universal and pre-established security safeguards that must be applied in relation to personal information that is collected by apps. The statutory requirement is that "personal information shall be protected by security safeguards appropriate to the sensitivity of the information" and the onus is placed on organizations to ensure that they have appropriate security safeguards in place.

Because the category of "legal apps" is so diverse, including a variety of tools with different functionalities and different uses of technical features, there is no single list of security safeguards that will be applicable to every app that under the legal apps umbrella.

In considering what security safeguards would be appropriate, the OPC has suggested that factors such as the sensitivity of the information, the amount of information, the extent of distribution, format of the information, and the type of storage be considered.

If there is a data security breach with your legal app, there are statutory notification requirements that you must comply with.

PIPEDA states that "personal information shall be protected by security safeguards appropriate to the sensitivity of the information" and places the onus on organizations to determine for themselves what safeguards are appropriate.

In the case of legal apps, the potential diversity of tools (both in terms of the functions they serve and the technology used) precludes a single list of security safeguards applicable to every app.

In thinking about security safeguards, legal app developers and providers should ensure that they have access to appropriate expertise as to what measures may be relevant in their circumstances. At a very general level, the OPC has proposed a list of factors to consider in choosing appropriate safeguards:

- *sensitivity of the information;*
- *amount of information;*
- *extent of distribution;*
- *format of the information (electronic, paper, etc.); and*
- *type of storage.*

For example, if you collect payment information including credit card data through your app, you will need to ensure that the communication and storage of this data meets appropriate security standards for sensitive information.

It should be noted that data security breach notification requirements require organizations to notify the Privacy Commissioner where there has been a security breach involving personal information "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." (s. 10.1 of PIPEDA). Organizations must also provide appropriate notification to individuals where a breach meets the real risk of significant harm threshold.

Organizations are required to document any security breaches involving personal information even if the incidents do not meet the threshold of harm required for reporting. This information must be retained for two years, and may be reviewed by the Privacy Commissioner.

12. What are the consequences to me and my organization if we do not comply with PIPEDA?

Brief Answer:

A breach of PIPEDA may lead a user to complain to the Privacy Commissioner of Canada, who can then conduct an investigation. If the matter is not resolved to the satisfaction of the parties, the Commissioner will issue a Report of Findings, which may include recommendations. Such recommendations are non-binding, but it is possible for either the Commissioner or the individual who complained to apply to the Federal Court for an order. If issued, a court order may require the organization to take certain steps to correct its privacy practices or pay damages. And, of course, court proceedings, including a ruling that an organization has breached PIPEDA, can have negative reputational consequences.

Individuals may complain to the Privacy Commissioner of Canada if they feel that their personal information has been dealt with in a way that infringes PIPEDA. Such a complaint will lead to an investigation. If the matter is not resolved to the satisfaction of the parties, the Commissioner will issue a Report of Findings. If a breach of PIPEDA is found, the Commissioner's Report may include recommendations. Although such recommendations are not binding, either the Commissioner or the complainant may apply to the Federal Court for an order. If issued, such an order may require the organization to take certain steps to correct its practices. The Court may also award damages. Court proceedings, including a ruling that an organization breached PIPEDA, can have negative reputational effects as well.

In addition to the recourse available under PIPEDA, breaches of privacy obligations may lead to lawsuits for negligence, breach of contract, breach of confidence, or intrusion upon seclusion. Data security breaches that have affected multiple individuals have also led to class action lawsuits

APPENDIX A: Developer Checklist

While developing technical features of app:

- Identify what personal information is needed to fulfill the app's functions and design the app with a view to only collecting this specific information.

- If you are using a pre-established platform to build your app, ensure that you understand what personal information will be collected and assess whether using this platform will interfere with your ability to appropriately protect your users' personal information.

- Consider the degree to which your app will involve communicating personal information to third-party services and be prepared to explain and account for this in your privacy policy.

- With respect to personal information being collected, consider whether anonymized or aggregate data is sufficient. Is de-identification at the point of collection possible?

- With respect to the collection of any sensitive personal information, consider using "just-in-time" notifications for users.

- Create adequate systems to delete information if a user withdraws his or her consent.

- Incorporate features that allow users to easily change their decisions regarding your app's treatment of their personal information once the app is installed.

- Adopt "privacy enabling" default settings.

- Ensure that you provide a level of security for personal information that is appropriate to the sensitivity of the personal information being collected.

    - In order to avoid accidental disclosure or intentional breach, consider using encrypted communications wherever possible and providing the option for two-factor authentication for account access.

- Consider whether your app provides legal information in a context (domestic violence, for example) where an "escape button" would be an important safety feature.

While developing materials and tools to obtain meaningful consent from users:

- Consider what information a user needs to know in order to provide meaningful consent. For example, ensure that you are sufficiently clear when describing what personal information is being collected and for what purpose(s), and with whom the personal information may be shared.

- In the case of legal apps consider what information that a user should know about:

    - whether a solicitor-client relationship is created; and

    - any potential risks that their personal information may be shared with law enforcement.

- Consider how best to share the above information with the user. As a baseline, draft and make available a privacy policy.

    - For mobile apps, consider the suggestions developed by the OPC for using visual cues such as layering the information, providing a privacy dashboard, and using graphics, colour and sound in order to obtain meaning consent in the mobile environment.

Ongoing matters relating to your organization:

- Designate an individual or individuals who are responsible for your organization's compliance with PIDEDA's Fair Information Practices.

- Create and follow procedures to address complaints and inquiries from users about the protection of their personal information.

- Ensure your employees are aware of and understand your organization's privacy practices and policies.

- Monitor security bug reports as well as any changes to the privacy policies of tools and services used by your app.

- Set time limits for data retention and follow them.

- Create and follow a data security breach protocol.

Works Referred to in this Document

Austin, Lisa M. and Lie, David and Sun, Peter and Spillette, Robin and D'Angelo, Mariana and Wong, Michelle, Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project (June 27, 2018). Available at SSRN: https://ssrn.com/abstract=3203601 or http://dx.doi.org/10.2139/ssrn.3203601

Edmonton Journal v. Alberta (Attorney General), [1989] 2 SCR 1326, 1989 CanLII 20 (SCC), <http://canlii.ca/t/1fszp>

Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principles, January 2018, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Office of the Privacy Commissioner of Canada, Interpretation Bulletin: Personal Information, October 2013, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/

Office of the Privacy Commissioner of Canada, Mobile Devices and Apps, December 14, 2018, https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/

Office of the Privacy Commissioner of Canada, Guidelines for Obtaining Meaningful Consent, May 2018, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

Office of the Privacy Commissioner of Canada, Guidelines on Privacy and Online Behavioural Advertising, December 2011, https://www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/gl_ba_1112/

Office of the Privacy Commissioner of Canada, Ten tips for a better online privacy policy and improved privacy practice transparency, November 2018, https://www.priv.gc.ca/en/privacy-topics/privacy-policies/02_05_d_56_tips2/

Office of the Privacy Commissioner of Canada, Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps, October 2012, https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/

Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009, https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/

Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 7 – Safeguards, January 8, 2018, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/

Personal Information Protection and Electronic Documents Act, SC 2001, c. 5, https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html