Canadian Journal of Law and Technology

Volume 18 | Number 1 Article 1

6-2020

Developing Privacy Best Practices for Direct-to-Public Legal Apps: Observations and Lessons Learned

Teresa Scassa
Faculty of Law, University of Ottawa

Amy Salyzyn
Faculty of Law, University of Ottawa

Jena McGill
Faculty of Law, University of Ottawa

Suzanne Bouclin
Faculty of Law, University of Ottawa

Developing Privacy Best Practices for Direct-to-Public Legal Apps: Observations and Lessons Learned

Teresa Scassa, Amy Salyzyn, Jena McGill and Suzanne Bouclin*

INTRODUCTION

Canada's access to justice problem is undeniable. Too many people are unable to get the help they need when they experience legal issues. The reasons underlying this problem are multi-faceted and complex. One major barrier to effectively accessing justice is the cost of legal services; the fees associated with hiring a lawyer are often prohibitive. Increasingly, technology is advanced as a potential solution to the unaffordability of conventional legal services. Courts have tried to create efficiencies by, for example, allowing for e-filing and video-conferenced testimony, where appropriate. For lawyers, new technology products emerge almost daily to help streamline tasks such as legal research, practice management, document creation and civil discovery processes. Indeed, Canadian law societies are now considering whether lawyers have a professional *duty* to be technologically competent. In addition to such developments in the courts and in lawyers' offices, there is a flurry of activity related to developing technological tools intended to be used directly by the public to address legal needs. For ease of reference, we will refer to such tools as "DTP (direct-to-public) legal apps."

As useful as they may be, DTP legal apps raise unique and important privacy issues. This article discusses a project we undertook with the goal of creating a set of privacy best practices for DTP legal apps. Our interest in privacy issues specific to legal apps dovetailed with the Office of the Privacy Commissioner of Canada's ("OPC") interest in encouraging the development of sector-specific guidance for compliance with privacy obligations. We obtained funding from the OPC to carry out this project in 2017 which resulted in a final report, *Improving Privacy Practices for Legal Apps: A Best Practices Guide,* submitted in March 2019. A full copy of this final report can be found in the Appendix. In this article, we detail our work on this project, including the challenges faced in fulfilling our

---

* Teresa Scassa is Canadian Research Chair in Information Law and Policy at the University of Ottawa; Amy Salyzyn is an Associate Professor at the University of Ottawa; Jena McGill is an Associate Professor at the University of Ottawa; and Suzanne Bouclin is an Associate Professor at the University of Ottawa. The authors gratefully acknowledge funding from the Contributions Program of the Office of the Privacy Commissioner of Canada ("OPC"). This funding supported the underlying research on a privacy best practices guide for the development of legal apps. The views expressed in this article are those of the authors and do not necessarily reflect those of the OPC.

research mandate (to draft a model privacy sectoral code for DTP legal apps) and the lessons we learned in that process.

Our goal here is twofold. First, we hope to provide the foundations for future projects and conversations relating to the optimal provision of DTP legal apps in Canada, and the development of privacy guidance for DTP legal app developers. Second, we provide critical reflections on the objective of creating a sectoral privacy code, particularly in a rapidly evolving technological context. Neither of these issues have yet been the subject of dedicated scholarly analysis. This article aims to fill this gap and facilitate more informed discussions about both the provision and regulation of DTP legal apps in Canada and privacy regulation in emerging digital spaces more generally.

In Part I, we outline the background and context of the project. In Part II, we discuss the feedback we received about privacy concerns and the best practices model from developers engaged in the creation of DTP legal apps. Part III considers how structuring the best practices guide through the lens of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[1] imposed specific, and sometimes problematic, constraints. In Part IV, we highlight some particular features of the DTP legal apps "sector" and identify how these realities impacted the development of what was initially conceived of as a sectoral privacy code. In Part V, we examine the role of law societies in relation to a privacy code of practice for DTP legal apps. In Part VI, we reflect on the final best practices guide we created. Finally, we revisit the lessons learned from this project.

I. Why Develop Privacy Best Practices for DTP Legal Apps?

We were motivated to develop privacy best practices specific to DTP legal apps because of issues that surfaced during a previous research project on legal apps conducted by three members of our team.[2]

One aspect of this earlier research involved creating an inventory of available legal apps in Canada. In both this previous research and in the privacy best practices project discussed here, we adopted a flexible and inclusive definition of "legal apps" as encompassing mobile and web-based resources that purport to assist individuals with legal tasks. In 2016, we inventoried approximately 60 legal apps available in Canada, which included apps meant to be used by lawyers as well as DTP legal apps.[3] We did not survey technologies that were directly embedded in the court system, such as e-filing or video-conferencing services.

---

1 *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5 [PIPEDA].

2 Jena McGill, Suzanne Bouclin & Amy Salyzyn "Mobile and Web-based Legal Apps: Opportunities, Risks and Information Gaps" (2017) 15 CJLT 229 [McGill, Bouclin & Salyzyn]. This research was funded by the Social Sciences and Humanities Research Council of Canada ("SSHRC") and was completed in 2016.

3 *Ibid* at 253-256.

Our inventory revealed that both public and private actors were responsible for legal app development in Canada, with a majority of apps created by private individuals working alone or in small teams.[4] Moreover, we noted that Canadian law schools were beginning to take on an important role in this arena by providing students with the training and opportunity to develop their own legal apps. Finally, we found that there has been some DTP legal app development by public actors such as public legal education organizations.[5]

The legal apps that we identified were diverse in their functions. Some provided legal information and advice, others assisted users in creating documents, others helped to streamline conventional legal processes and assisted in collecting evidence.[6] For example:

- **Legal information:** *Drone Zone Canada* (alerts users to zones where personal drones cannot be flown, according to Federal Regulations);[7] *Bardal Factors* (assists in assessing how much notice or pay in lieu of notice an employer must give to an employee upon termination of employment);[8]
- **Document creation:** *My Legal Briefcase* (helps "ordinary people to handle their cases with or without a lawyer" and provides assistance "in preparing simple legal documents");[9] *Ontario Small Claims Wizard* (currently in development, will guide people through the small claims process by advising users on which documents they need to file and facilitating on-line completing of those forms);[10]
- **Streamlining conventional legal processes:** *ParDone* (an "online platform that reduces the time, cost, and complexities of the criminal record suspension process");[11] *Thistoo* ("personal divorce assistant" walks users through the necessary steps of an uncontested divorce in Ontario);[12]

---

4 *Ibid* at 234.

5 *Ibid* at 236-237.

6 *Ibid* at 253-263.

7 Apple Store, "Drone Zone Canada" (accessed 11 December 2019), online: < https://itunes.apple.com/ca/app/drone-zone-canada-restricted-airspace-finder/id1231448891?mt = 8 > .

8 "Bardal Factors" (accessed 11 December 2019), online: < http://www.bardalfactors.ca/whats-reasonable > [Bardal].

9 "My Legal Briefcase" (no longer active), online: < https://www.mylegalbriefcase.com/ > . An archived version is available via the Wayback Machine (18 January 2019), online: < https://web.archive.org/web/20190118114814/https://www.mylegalbriefcase.com/ > .

10 "Small Claims Wizard" (no longer active), online: < http://www.smallclaimswizard.-com/ > . An archived version is available via the Wayback Machine (5 May 2019), online: < https://web.archive.org/web/20190118064350/https://smallclaimswizard.-com/ > .

11 Legal Innovation Zone, "ParDONE" (accessed 11 December 2019), online: < https://pardone.ca/about-us.html >

12 "Thistoo" (no longer active), online: < https://thistoo.co/ > . An archived version is

- **Evidence creation:** *LegalSwipe* (aims to inform people of their rights during a police stop and can also "send emergency contacts a personalized message with ongoing updates of [one's] geographic location" and "record audio and video to be e-mailed to emergency contacts and uploaded to synchronized Dropbox accounts").[13]

In the three years since our initial research, the legal apps landscape in Canada has continued to shift, with new legal apps appearing regularly, while others have been discontinued.[14]

Our earlier study also provided an analysis of policy issues raised by this technology and concluded that legal apps present a range of opportunities for improving access to justice in Canada.[15] For instance, they may play a part in mitigating the financial, psychological, informational and physical barriers associated with traditional legal services. We observed that DTP apps can play a promising role in furthering access to justice, and that "[i]n particular, apps that allow individuals to generate legal documents, like contracts or wills, without retaining a lawyer or with reduced assistance from a lawyer, have the potential to increase public access to certain legal services at significantly lower costs."[16]

In addition to identifying access to justice opportunities presented by legal apps, our 2016 study also identified some significant risks.[17] Specifically, we identified privacy risks as one core concern associated with the proliferation of legal apps in Canada and we considered these risks most salient in the case of DTP legal apps.[18] For example, when users engage with DTP legal apps that provide legal information or help them create legal documents, there is a danger that users could mistakenly believe that any personal information they share will receive special protection due to solicitor-client privilege.[19] The degree of such

---

available via the Wayback Machine (28 October 2017), online: <https://web.archive.org/web/20171028035415/https://welcome.thistoo.co/>.

13 Legal Innovation Zone, "Legalswipe" (accessed 11 December 2019), online: <http://www.legalinnovationzone.ca/startup/legalswipe/>.

14 For newly developed DTP legal apps, see, e.g., *Om* (allows users to "create a legal will and emergency care plan, estate plan, and assign a power of attorney online. . .in 20 minutes") (accessed 11 December 2019), online: <https://omcompany.com/> [Om]; and *Destin.Ai* (assists with various immigration documentation such as work permits, visitor visas and citizenship documentation) (accessed 11 December 2019), online: <https://destin.ai/>. At the same time, some legal apps have been discontinued, e.g. the *Thistoo* application mentioned above, which previously assisted individuals with uncontested divorce applications. For an updated inventory of DTP legal apps see: Amy Salyzyn, William Burke and Angela Lee, Direct to Public Legal Digital Tools in Canada: A Draft Inventory, online: <https://techlaw.uottawa.ca/direct-public-legal-digital-tools-canada>

15 McGill, Bouclin & Salyzyn, *supra* note 2 at 240-251.

16 *Ibid* at 241.

17 *Ibid*.

18 *Ibid* at 244-246

19 *Ibid* at 246.

risk will no doubt depend on the nature of the legal app. It may be extremely unlikely that a member of the public who is using a legal dictionary provided on a mobile app to look up legal terms will believe that their search terms will be protected by solicitor-client privilege. The risk of such a mistake would seem much higher, however, in the case of a legal app that requests that users type in the details of their legal problem in order to connect them with a lawyer. A user of this type of app may indeed not understand that the information she provides when using this tool might not receive the stringent confidentiality protections that it otherwise would have received if she had provided such information in person to a lawyer.

DTP legal apps also raise heightened privacy concerns because they are likely to collect information that may be uniquely sensitive. For example, the simple fact that a user is consulting a legal app about initiating divorce proceedings or obtaining a criminal pardon may be sensitive personal information. Likewise, apps that help users collect evidence—such as "police encounter" apps that include audio and video-recording functions—are likely to be gathering sensitive information. Additionally, the information collected by these "police encounter" apps, and other kinds of DTP legal apps, could be of interest to third parties, who might request or compel the disclosure of this information. For instance, apps that assist individuals in resolving legal disputes outside of court may collect information—including financial information—that could be discoverable to an opposing party if the matter proceeds to civil litigation.

Potential use and misuse of personal information by a commercial third party is a further concern with DTP legal apps. In our 2016 study, we found privacy concerns specific to health apps to be instructive in analyzing similar issues in the legal apps context:

> In the health care context [. . .] many of the companies who produce wearable fitness products, like *Fitbit,* reserve rights to the data they collect. This enables the companies to commercially share the data, analyze it, provide the information to government authorities and/or dispose of the data as an asset in the event of a bankruptcy or corporate merger. User data can thus be shared or sold to third parties for purposes unrelated to the specific mandate of the app, like advertisers, insurance companies, or drug companies.[20]

More recently, researchers from the Institute for Science, Law and Technology at Chicago-Kent College of Law, analyzed the privacy policies and permissions of hundreds of health apps. They found that "over 70% of the medical apps. . . studied shared users' sensitive information with third party data aggregators, without the users' knowledge or consent."[21]

---

[20] Jena McGill, Suzanne Bouclin, Amy Salyzyn & Karin Galldin, *Emerging Technological Solutions to Access to Justice Problems: Opportunities and Risks of Mobile and Web-based Apps* (Report submitted to SSHRC, October 2016), online: <https://commonlaw.uottawa.ca/sites/commonlaw.uottawa.ca/files/ksg_report_-_mcgill_et_al_oct_13_final_-to_send_to_sshrc.pdf> at 18 (internal footnotes omitted) [McGill et al., SSHRC].

There is reason to worry about similar practices when it comes to DTP legal apps. Personal information is a hot commodity for targeted advertising and DTP legal apps have the potential to collect personal information about consumers' needs for legal or other services based upon the conflicts, challenges or legal issues they disclose to the app. DTP legal apps may also collect data that is of interest to specific industries. For example, real estate agents may want to obtain the contact information of individuals getting divorced or who are planning to immigrate to Canada; financial planners may want to gather similar information for those drafting wills; and criminal defence lawyers could benefit from targeted advertising to individuals who have been recently detained by police. Indeed, in the course of our consultations on privacy issues faced by DTP app developers, we learned that one DTP legal app developer had, in fact, been directly approached by actors from other industries seeking to acquire user data collected by the developer's app.

Given the promise of DTP legal apps to facilitate access to justice, and the associated privacy risks, in 2017 we applied for and received funding from the OPC Contributions Program to develop a Privacy Code of Practice for mobile and web-based legal apps intended for use by the public.[22] The OPC's Contributions Program involves an annual call for proposals for research relating to the OPC's mandate under PIPEDA.[23] PIPEDA is the federal data protection statute that applies to the collection, use and disclosure of personal information in the course of private sector commercial activity in most of Canada.[24]

In embarking on this two-year project, it was important for us to provide guidance that was relevant and practical for legal app developers in Canada. To this end, we took significant steps throughout the project to consult a range of legal app developers, as well as other stakeholders from legal practice, the academy and civil society. The best practices guidance that we ultimately developed went through many iterations before reaching its final form. The feedback we received on different drafts, from developers and privacy experts, has been invaluable. The next section focuses on the feedback that we received from developers.[25]

---

[21] Lori Andrews, "A New Privacy Paradigm in the Age of Apps" (2018) 53 Wake Forest L. Rev. 421 at 421.

[22] The 2017-2018 call for proposals for the Office of the Privacy Commissioner's Contributions Program indicated the OPC's interest in the creation of sectoral codes: Office of the Privacy Commissioner of Canada, *2017-2018 Departmental Plan* (2017), online: https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2017-2018/dp_2017-18/ [OPC Dept Plan 2017-18].

[23] Office of the Privacy Commissioner of Canada, "About the Contributions Program" (14 December 2018), online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/about-the-contributions-program/ > .

[24] PIPEDA, *supra* note 1.

II. Developer Responses to our Project

Throughout this project, developer input was essential to enriching our understanding of the DTP legal app sector and for testing the practicality of our ideas. We held a closed workshop in October 2017, which included a number of legal app developers as well as privacy experts, legal academics, and policy professionals. We also met and consulted over email with developers outside of this meeting and with those supporting app development at law schools and in technology incubators.

We learned a considerable amount from these interactions. In the first place, developers indicated that there were generally very low levels of awareness of privacy issues arising from legal apps and of the relevance of PIPEDA in legal innovation spaces. One reason for this may be that many DTP legal app developers are working as individuals or in small teams with a singular focus on addressing a particular access to justice issue. Consideration of privacy issues and compliance is not necessarily a regularized feature of the development process in this environment. This may particularly be the case in law school courses on app development, and in legal hackathons. In recent research on legal apps designed for non-lawyer use in the United States, Rebecca Sandefur observes that "[d]evelopment of digital tools is usually provider-driven, reflecting the interests and beliefs of those offering the service, rather than the wants and needs of the intended user populations."[26] Accordingly, privacy issues might tend to take a back seat; a developer who is interested primarily in addressing an access to justice issue through his or her app may simply not be thinking about privacy needs of the intended users. The developers also confirmed that there is no existing best practices guidance in relation to privacy practices in the DTP legal apps context.

To our team, this feedback confirmed the value of creating an "entry-level" guidance document that could assist DTP legal app developers in understanding and meeting their privacy obligations. Indeed, one core benefit of privacy guidance might be awareness-raising: a document about privacy best practices geared specifically to DTP legal app developers offers a starting point to increase developer knowledge about privacy issues at the app-design stage. Addressing privacy issues at the design stage (known as "privacy by design")[27] is a best practice, but it of course requires appreciation of the privacy issues at stake.

---

[25] Ethics approval was sought and obtained from the University of Ottawa's Research Ethics Board (Ethics Certificate #06-16-14) to engage in these consultations and refer to the feedback received in future publications.

[26] Rebecca Sandefur, *Legal Tech for Non-Lawyers: Report of the Survey of US Legal Technologies* (Chicago: American Bar Foundation, 2019), online: < http://www.americanbarfoundation.org/news/3137 > [Sandefur].

[27] See, e.g., Ann Cavoukian, "Privacy by Design: The Seven Foundational Principles" (Toronto: Information and Privacy Commissioner of Ontario, January 2011), online: < https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf > [Cavoukian].

At the same time, developers felt strongly that, if respecting user privacy is seen as overly burdensome, a document outlining privacy issues and obligations might discourage app innovation that is otherwise in the public interest. We were warned against complicating design and implementation issues. Developers revealed concerns about the usability of their apps, and may be frustrated by privacy considerations that either complicate the design or make the app less user-friendly. We also heard concerns that highlighting the need for compliance with privacy obligations could be seen as calling into question whether particular DTP legal apps are complaint with the law, potentially undermining the confidence of developers and those funding or supporting their work.

While the developers we consulted were open to, and interested in, receiving privacy guidance, the feedback we received on the drafts of our guide revealed concerns about the burdens of compliance. Developers wanted concise, clear direction about what to do to meet privacy obligations in creating a legal app; for example, they suggested checklists as a useful tool. Layered guidance was also suggested, with simple statements up front and the option for developers to click through for additional details or explanations. Some even suggested that the privacy guidance itself should be in the form of an app. However, the diversity of DTP legal apps, including their differing goals, functionalities, target users and kinds and quantity of information collected, made simple, "one-size-fits-all" compliance statements impossible. In addition, some of the concepts at the core of privacy law are themselves vague and varied. These include the definition of personal information, determining what is or is not sensitive personal information, determining whether PIPEDA applies, and deciding what level of consent is required in a given set of circumstances.

This tension between a desire for guidance and a fear that an overly restrictive model would hamper innovation reflects a couple of phenomena that are not exclusive to DTP legal app development but that certainly seem to be in play in this context. First, legal compliance issues are often dealt with on the business end of things; that is, when an app is commercialized. However, many DTP legal apps are developed by individuals or teams who are looking for technological solutions to real-world problems, often with altruistic rather than commercial motivations. Genuinely free legal apps are not even subject to PIPEDA.[28] Strictly speaking, legal compliance becomes an issue only once a decision is made to commercialize an app. This might happen once the app becomes a success, but it may also arise when the developer realizes that the cost of maintaining the app will require some form of revenue stream. Because DTP legal apps may be specific to the laws of a particular jurisdiction (such as a province) and because the subset of individuals that face the relevant legal issues within that jurisdiction will be smaller still, DTP legal apps may be difficult to make profitable simply through a fee for downloading the app. It may therefore become necessary for app developers to contemplate monetizing the information

[28] 'Free' in this sense would mean apps that do not generate revenue through download fees, advertisements, or the selling of data.

collected by the app to maintain the app or take it to the next level. Thus, a significant challenge is that the need for compliance with PIPEDA may arise sometime after the actual development of the app, with different players and interests at stake. Commercialization might also change what information is collected, used or disclosed—for which purpose, and to whom.

In our guidance document, we recommend building privacy into app design even if there is no commercial plan for the app, simply because a failure to do so may present problems if commercialization is ultimately pursued. We also emphasize that, even if an app is never commercialized and PIPEDA never applies, users stand to benefit when a developer chooses to enhance transparency around privacy practices and takes measures to better protect personal information.

To be sure, the feasibility of adopting any particular privacy-enabling feature will be impacted by the cost of adoption and the resources available to the development team. In presenting best practices to developers as opposed to a detailed prescriptive code of requirements, we aimed to inform developers about important privacy principles while leaving open to them a variety of routes to comply with such principles. On the issue of cost we would also note: (1) not all privacy-enabling choices involve an additional financial cost (for example, limiting collection of personal data); (2) addressing privacy issues upfront can be considerably more cost-effective them "bolting them on" after-the-fact; and (3) there can be financially beneficial reputational advantages to building strong privacy enabling features into a product.[29]

III. How PIPEDA Shaped the Best Practices Guide

The nature and source of our funding—the OPC Contributions Program—meant that the lens through which we analyzed the privacy issues raised by DTP legal apps and the guidance provided to developers, was that of PIPEDA. While PIPEDA is the federally-enacted data protection statute that applies to the collection, use and disclosure of personal information in the course of private sector commercial activity in most of Canada, its application is complicated by Canadian federalism.[30] PIPEDA applies to the federally-regulated private sector; it also applies to the private sector more broadly in any province that has not enacted legislation that is found to be "substantially similar."[31] Three provinces have such legislation for the general private sector.[32]

---

[29] For further discussion see, e.g., Cavoukian, *supra* note 27; Deloitte Canada, "Ryerson, Deloitte Partner to Offer Privacy Certification" (2019), online: < https://www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html > ("Treating privacy as a business issue avoids the risk of reputational damage should a privacy violation occur, and it is much easier and more cost-effective to build the right privacy and security defaults into a new technology from the outset than have to introduce costly retrofit").

[30] For a discussion of the constitutional issues relating to the application of PIPEDA, see Teresa Scassa & Michael Deturbide, *Electronic Commerce and Internet Law in Canada*, 2nd ed. (Toronto: Wolters Kluwer, 2012) at 89-92.

In those provinces, their own legislation will apply to the *intra*-provincial collection, use or disclosure of personal information in the course of commercial activity by provincially regulated businesses, although the applicable principles are substantially similar to those in PIPEDA. *Inter*-provincial and other cross-border collection, use or disclosure will still be under PIPEDA's purview.[33] Further, some legal app development, such as smart court or tribunal forms, takes place within the provincial and federal public sectors. These apps would not be subject to PIPEDA, but to the relevant public sector freedom of information and protection of privacy legislation. Although basic privacy principles are shared across jurisdictions in Canada as well as across public and private sectors, our guidance to DTP legal app developers had to use PIPEDA's varied applicability as a starting point, even if just to let developers know which Commissioner's office to turn to for further information.

The question of PIPEDA application added a layer of complexity to our task. For instance, PIPEDA applies only to personal information collected, used and disclosed in the course of *commercial activity*. The link to commercial activity is crucial to determining whether PIPEDA should apply to the tools that DTP legal app developers are working on. Some of the developers we consulted found the discussion about PIPEDA application frustrating. As noted above, many legal apps intended for public use are developed by groups or individuals whose priority is to improve access to justice and who are not concerned about commercialization. Linking privacy best practices to commercialization is thus not intuitive for many developers in this sector. We emphasize in our guidance document that compliance with privacy principles is important even if commercialization is not a primary goal; nevertheless, the fact that PIPEDA applies only to commercial activity is problematic in the DTP legal apps domain, where a significant number of apps are not commercial—at least at the outset.

A related issue is that we approached privacy compliance by focusing on the Fair Information Principles ("FIPs") that form PIPEDA's normative core.[34]

---

[31] PIPEDA, *supra* note 1 at ss. 4, 26(2)(b). For further discussion, see also Office of the Privacy Commissioner of Canada, "Provincial Legislation Deemed Substantially Similar to PIPEDA" (29 May 2017), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/>

[32] *An Act respecting the protection of personal information in the private sector*, C.Q.L.R. c. P-39.1 (QC); *Personal Information Protection Act*, S.B.C. 2003, c. 63 (B.C.) [B.C. PIPA]; *Personal Information Protection Act*, S.A. 2003, c P-6.5 (Alberta). The relevant exemption orders are: *Organizations in the Province of Quebec Exemption Order*, SOR/2003-373; *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220; and *Organizations in the Province of Alberta Exemption Order*, SOR 2004-219.

[33] Office of the Privacy Commissioner of Canada, "Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts" (5 November 2004), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/>.

These principles are helpful in identifying key considerations for developing apps that are compliant with data protection best practices. Indeed, the FIPs are at the heart of the substantially similar provincial statutes in Quebec, Alberta, and British Columbia. However, certain privacy concerns unique to DTP legal apps—including, for example, the issue of whether a solicitor-client relationship is created between a user and an app—do not fit easily within a FIP-focussed approach. This does not mean that these concerns cannot be addressed in DTP legal app-specific guidance—in fact, we include them in our guidance document—however, it does mean that our starting point in defining and addressing privacy and the key elements of privacy protection was different from what it might have been had our approach been less PIPEDA-centric.

Additionally, the "notice and consent" model of protecting user privacy, which is embedded in PIPEDA and the FIP-focused approach, had some significant limitations in addressing privacy issues raised by DTP legal apps. In principle, data subjects must be given notice of any data collection and its purposes prior to its taking place, and they must have an opportunity to consent to the collection. The concepts of both notice and consent need to be re-considered in order to be meaningful in digital contexts.[35] For example, in our 2016 research we found that, although detailed privacy policies are a favoured method of telling users how their information will be used and stored, multiple studies demonstrate that this technique is an ineffective means of obtaining meaningful consent in the digital context.[36] For example, a study of fitness apps concluded that the apps' privacy policies and terms of service tended to be "opaque, unclear, misleading, and even contradictory."[37] The authors of this study observed that fitness apps' terms of service often did not disclose the duration of data retention or with whom data is shared.[38] Even if privacy policies and terms of service are completely clear, concerns about obtaining meaningful consent linger due to user disengagement. A 2016 study found that 98% of study participants agreed to sign fictional terms and conditions to access a fictional

---

[34] Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principles" (May 2019), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/>.

[35] The OPC has issued new guidance in an attempt to address the growing challenges of obtaining adequate consent in the rapidly expanding digital context: Office of the Privacy Commissioner of Canada, "Guidelines on Obtaining Meaningful Consent" (May 2018), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ [OPC Guidelines]. These Guidelines took effect 1 January 2019.

[36] McGill et al., SSHRC, *supra* note 20 at 18-19.

[37] Andrew Hilts, Christopher Parsons & Jeffrey Knockel, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security" Open Effect Report (2016) at 49, online: <https://openeffect.ca/reports/Every_Step_You_Fake.pdf> [Hilts et al.].

[38] *Ibid* at 45-47.

website notwithstanding the inclusion of a clause requiring users to give up their first born child as a form of payment.[39] Given these realities, our guidance draws specifically on existing work by the OPC on developing better online privacy policies and obtaining meaningful consent in the mobile app context.[40] Specifically, we encourage DTP legal app developers to supplement privacy policies with techniques such as privacy dashboards[41] and pop-up windows to provide timely notice to users about the collection of information and other privacy related matters.

An additional challenge in addressing privacy issues in the DTP legal app context stems from the line between the user and the app developer, in terms of information collection, use and disclosure being neither straight nor necessarily clear. In order to build apps, developers rely, as a general matter, on pre-existing platforms or third-party code. It is simply not feasible or sensical to "build everything from scratch" each time a new app is developed. Privacy-related problems can arise, however, because certain tools may collect personal information from users in a manner that is not necessary for the operation of the app and that is not disclosed to users. Indeed, recent studies, which are discussed in more detail below, demonstrate that even sophisticated developers are not always aware of the resulting disclosures to third parties.

An example of how using third-party code can complicate compliance with privacy regulations can be found in a recent study conducted by Lisa Austin and several co-authors.[42] The Austin et al. study involved the creation and use of a tool to "compare the declared data practices of mobile apps to their actual (or

---

[39] Jonathan A. Obar and Anne Oeldorf-Hirsch, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services" (Paper from TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016), online: <https://ssrn.com/abstract=2757465> or <http://dx.doi.org/10.2139/ssrn.2757465>.

[40] See, e.g., Office of the Privacy Commissioner of Canada, "Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency" (November 2018), online: <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), online: <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/> [OPC Good Practices]. See also OPC Guidelines, *supra* note 35.

[41] A privacy dashboard is a single location through which users can view and control multiple privacy settings. Dashboards "allow users to gain insights and exercise control over data that a digital service provider has accumulated about them": Johana Cabinakova, Christian Zimmermann & Guenter Mueller, "An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case" (Association for Information Systems Research Papers no 114, 2016). The OPC recommends dashboards as a meaningful way to protect and enhance the privacy of app users: see, e.g., OPC Good Practices, *supra* note 40.

[42] Lisa M. Austin et al., "Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project" (2018), online: <https://ssrn.com/abstract=3203601> or <http://dx.doi.org/10.2139/ssrn.3203601> [Austen et al.].

potential) practices in order to flag potential discrepancies."[43] In short, the tool: (1) used "AI techniques" to automate and thus quickly read privacy policies of hundreds of Android apps; (2) then conducted a "[scan] and analysis of an app's static code in order to determine what the potential permissions are in relation to personal data collection" and (3) finally compared (1) and (2) to identify "potential personal data collection practices that are not declared in the relevant privacy policy."[44] The study found what it termed as a "fairly high" level of non-compliance among the applications studied: 59.5% had discrepancies between the data practices declared in their privacy policy and what the app was actually doing.[45] The authors further concluded that the discrepancies were "often the result of undeclared collection of personally identifiable information by third party code used by the developer, rather than code written by the developer themselves."[46] An example of how this might occur, as discussed in the study, is with the use of "ad libraries":

> An app developer who wants to serve ads to its users will install an ad library from an ad network. This ad library allows the app to "call" an ad network and have an ad delivered to a user and displayed within the app. The ad network, which has many participating companies, decides on which particular ad from which company will be delivered to a particular user.
>
> It is the ad network, not the app, that engages in the consumer profiling needed to make this kind of targeted advertising work. This is what leads to potential privacy problems. If an ad network simply wanted to deliver an ad to an app, its ad library would not need access to Android permissions such as the device ID. In order to target the ads, the ad library needs to retrieve information about the user and send this off device to the ad network's servers.
>
> . . . 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.[47]

---

[43] *Ibid* at 2.

[44] *Ibid* at 2

[45] *Ibid* at 2.

[46] *Ibid* at 2.

[47] *Ibid* at 24-25.

When practices like those described in the above paragraph are not disclosed to users, privacy compliance issues arise. PIPEDA compliance requires appropriate notice and consent for the collection, use and disclosure of personal information. Incomplete or inaccurate information about such practices is, consequently, not PIPEDA-compliant. With respect to the issue of behavioural advertising in particular, Austin et al. conclude "there is a strong argument that Canadian privacy law requires opt-out consent for mobile behavioural advertising" and that there are "serious reasons to think that many apps are failing [to provide adequate information about these practices]."[48]

Recently, there has also been considerable study of undisclosed data disclosures to third parties resulting from developer use of Facebook's Software Development Kit ("SDK"). Facebook's SDK is, in basic terms, "a set of software development tools that help developers build apps for a specific operating system."[49] For example, in one study published by Privacy International in December 2018, researchers found that some of the most widely used apps in the Google Play Store (like, for example, Yelp and Duolingo) were automatically sending personal data to Facebook at the moment that they were activated and that they were doing this even if the user did not have a Facebook account.[50] The researchers also found that the data transmitted included unique identifiers that could be used to create detailed user profiles and that some user-privacy controls purported to give users control over data sharing without actually doing so.[51] In more practical terms, the Privacy International study described the impact of this activity as follows:

> For example, an individual who has installed the following apps that we have tested, "Qibla Connect" (a Muslim prayer app), "Period Tracker Clue" (a period tracker), "Indeed" (a job search app), "My Talking Tom" (a children's' app), could be potentially profiled as likely female, likely Muslim, likely job seeker, likely parent.[52]

Several months after the publication of its report, Privacy International retested all the apps and found that "a number of apps no longer transfer personal data to Facebook the moment a user opens the app" but also that "many apps still exhibit the same behaviour we described in our original report."[53]

---

48 *Ibid* at 26.

49 Privacy International, *How Apps on Android Share Data with Facebook* (London, UK: December 2018), online: <https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf> at 3 [Privacy International Dec 2018].

50 *Ibid;* Privacy International, "Guess What? Facebook Still Tracks You on Android Apps (Even if You Don't Have a Facebook Account" (5 March 2019), online: <https://privacyinternational.org/blog/2758/guess-what-facebook-still-tracks-you-android-apps-even-if-you-dont-have-facebook-account>.

51 Privacy International Dec 2018, *supra* note 49 at 3-4.

52 *Ibid* at 4.

53 Privacy International, "Investigating Apps interactions with Facebook on Android"

The *Wall Street Journal* published an article in February 2019 that detailed its own study that similarly found Facebook was "collect[ing] intensely personal information from many popular smartphone apps just seconds after users enter it, even if the user has no connection to Facebook."[54] The article reports, for example:

> In the Journal's testing, Instant Heart Rate: HR Monitor, the most popular heart-rate app on Apple's iOS, made by California-based Azumio Inc., sent a user's heart rate to Facebook immediately after it was recorded.
>
> Flo Health Inc.'s Flo Period & Ovulation Tracker, which claims 25 million active users, told Facebook when a user was having her period or informed the app of an intention to get pregnant, the tests showed.
>
> Real-estate app Realtor.com, owned by Move Inc., a subsidiary of Wall Street Journal parent News Corp, sent the social network the location and price of listings that a user viewed, noting which ones were marked as favorites, the tests showed.
>
> None of those apps provided users any apparent way to stop that information from being sent to Facebook.[55]

Shortly after the *Wall Street Journal* published this article, it issued a follow up article to note that several of the apps studied "issued updates to cut off transmission of sensitive data to Facebook."[56]

While the reporting of issues relating to Facebook's SDK seems to have resulted in some changed practices, the studies mentioned above stand, at the very least, as concerning cautionary tales about the potential ubiquity of apps engaging in undisclosed data sharing with third parties. It also demonstrates how the current apps environment poses an uneasy fit with conventional privacy regulation, which generally conceives of privacy dynamics arising directly between a user of a product or service and the provider of the product or service.[57] Under this conventional framework an app provider is generally accountable for the personal information that its app collects, uses, and discloses,

---

(December 2018, updated March 2019), online: <https://privacyinternational.org/campaigns/investigating-apps-interactions-facebook-android>.

[54] Sam Schechner & Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook" *Wall Street Journal* (22 February 2019), online: <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>.

[55] *Ibid.*

[56] Sam Schechner, "Popular Apps Cease Sharing Data With Facebook" *Wall Street Journal*, (24 February 2019), online: <https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791>.

[57] We acknowledge Lisa M. Austin's insights on this point in her talk as part of a panel on

but not for information collected, used or disclosed by others. The current realities in digital space, including the extent to which data is regularly shared with third parties in ways that are often not transparent or even discoverable to users, has generated new privacy dynamics and concerns that need to be accounted for.

To be sure, the regulatory landscape has been evolving to some extent to take into account this new reality. As the OPC's recent Report of Findings into a complaint against Facebook shows, the sharing of personal data between platforms and apps may well amount to a disclosure that is subject to PIPEDA.[58] Notice of and consent to such disclosures would therefore be required, and the disclosures would have to be ones that "a reasonable person would consider are appropriate in the circumstances."[59] Real questions remain, however, as to whether our current approaches to privacy regulations are sufficiently up to the task of protecting users in the current digital context.

An additional complicating layer is that legal app developers may not know or understand how information is being shared with and used by third parties when they employ pre-existing platforms or third-party code. In response to the Privacy International study mentioned above, for example, one app provider stated that it was "not aware" that it had been sending data without user consent.[60] Similarly, as reported in yet another study of the issues surrounding the use of Facebook SDK, there appeared to be a general lack of understanding among developers about what Facebook SDK was doing.[61] In this study, conducted by the German mobile security initiative Mobilsicher, researchers reported that most of the developers who they asked about the data practices arising from the use of Facebook's SDK wrongly assumed that the information that Facebook would be receiving was anonymous, when it was in fact not.[62] Although Austin *et al* did not directly question app developers about this issue for their study, they also point to lack of awareness being a major issue: "[w]e can surmise that similar to how end users often do not read the privacy policies of the

---

privacy and legal apps held at the University of Ottawa, Faculty of Law (25 February 2019).

58 Office of the Privacy Commissioner of Canada, "Joint Investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia," PIPEDA Report of Findings #2019-002 (25 April 2019), online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/ > .

59 PIPEDA, *supra* note 1, s. 5(3).

60 Madhumita Murgia, "Popular Apps Dhare data With Facebook Without User Consent" *Financial Times* (20 December 2018) < https://www.ft.com/content/62f74704-0abf-11e9-9fe8-acdb36967cfc > .

61 Miriam Ruhenstroth, "How Facebook Knows Which Apps You Use—and Why This Matters" *Mobilischer* (13 December 2018), online: < https://mobilsicher.de/hintergrund/how-facebook-knows-which-apps-you-use-and-why-this-matters > .

62 *Ibid.*

applications they use, application developers do not read or properly incorporate the privacy policies of 3rd party libraries and tools they use to build their applications."[63]

If lack of awareness is, indeed, a significant issue, this points to the potential need for "transparency-enhancing technologies" ("TETs") that can help users—or developers—map data flows. For example, Austin *et al* note that the type of tool which they used to compare declared data practices of apps to their actual practices could also be used by developers to help them "detect potential privacy problems with their apps by flagging for them unforeseen informational consequences of their designs."[64] To be sure, the usefulness of any such tool to developers and, in particular, small DTP developers, will depend on its affordability and its availability (the actual tool used by Austin et al. is a described by the researchers as a prototype and is not available for public use).

IV. A "Sectoral" Code for DTP Legal Apps

Some of the privacy issues raised by DTP legal apps are similar or identical to privacy issues raised by all apps. In considering developing privacy best practices for DTP legal apps, we noted the guidance already developed by the Federal Commissioner as well as some provincial Commissioners (Alberta and British Columbia namely) in relation to mobile apps.[65] As detailed in Part I of this article, our project began from the premise that there is something unique about DTP legal apps that raises issues requiring special consideration, not unlike the issues that health-related apps may raise.[66] As detailed in Part II of this article, throughout the course of this project we received feedback from developers that made it clear that many DTP legal apps are being created without much concern about, or awareness of, privacy issues. For these reasons, we felt that specific guidance for DTP legal app developers would be a useful contribution. As noted above, the impetus for the project grew from a prior research study that looked at legal apps specifically, and this necessarily shaped the parameters of our privacy project; we conceived of DTP legal apps as a distinct sub-category of apps based on the intended users, the sensitive nature of the personal information that might be shared via the app, and the potential relationship between some app functionalities and provincially or territorially regulated legal services.

The OPC has previously shown interest in the development of sector-specific codes.[67] In fact, in this round of its Contributions Program, it funded both our

---

[63] Austin et al., *supra* note 42 at 17.

[64] *Ibid* at 5, 10.

[65] OPC Good Practices, *supra* note 40.

[66] For example, the American Medical Association has collaborated with the company Xcertia for the development of guidance on the development of mobile health apps: Xcertia, "mHealth App Guidelines" (12 August 2019), online: <https://www.xcertia.org/the-guidelines/>.

project and another one aimed at developing a sectoral code of practice for autonomous vehicles.[68] Similarly, the European Union's *General Data Protection Regulation* ("GDPR")[69] recognizes a role for sectoral codes of practice. Article 40(1) of the GDPR states:

> 40(1). The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

In addition, paragraph 40(2) anticipates that associations and other representative bodies may develop such codes.[70] The GDPR provides for the supervisory bodies within individual member states (privacy commissioners) to review such codes and to approve them if they meet specified standards. The supervisory body can register and publish approved codes. Unlike the GDPR, while section 24(c) of PIPEDA authorizes the Commissioner to "encourage organizations to develop detailed policies and practices, including organizational codes of practice," nothing provides a mechanism for the formal endorsement of any sectoral code.

Our project fits squarely within the high-tech sector of the economy, and to some extent, the challenges we experienced in developing a code of practice reflect certain characteristics of that sector. A key feature is the extent to which technology is breaking down traditional concepts of "sectors" from the perspective of privacy law. Past sectoral codes focussed on specific activities, such as direct marketing to consumers,[71] banking or financial services,[72] or insurance services.[73] On the one hand, our project addressed legal services

---

67 See OPC Dept Plan 2017-18, *supra* note 22.

68 Rajen Akalu, "Developing a Privacy Code of Practice for Connected and Automated Vehicles" (2019) 17 C.J.L.T. 306 [Akalu].

69 *General Data Protection Regulation*, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, [2016] OJ L 119.

70 *Ibid* at art. 40(2).

71 For example, the Canadian Marketing Association has an ethical code that addresses privacy issues: Canadian Marketing Association, "CMA Code of Ethics and Standards of Practice" (October 2019), online: <https://www.the-cma.org/regulatory/code-of-ethics>.

72 The Canadian Bankers Association established a privacy code of conduct in 1986. This code was discontinued after the coming into effect of PIPEDA: Canadian Bankers Association, "Banks and Your Privacy" (29 March 2011), online: <https://cba.ca/banks-and-your-privacy>.

73 See, e.g., Canadian Bankers Association, "CBA Code of Conduct for Authorized Insurance Activities" (2003), online: <https://cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/vol_20090000_authorizedinsuranceactivities_en.pdf>.

(defined broadly to include more than what is encompassed by the jurisdiction of the regulated legal profession), but it did so with the qualification that it was aimed at legal apps—in other words, at the technologically enabled delivery of legal services, tools, and information. As a result, many of the privacy issues raised by DTP legal apps are not confined to the legal services "sector," rather they are a function of the underlying technology of apps.[74] Thus, many of the privacy issues raised by app technologies are common to all applications of these technologies. This made the subject matter of the guidance exceptionally broad in some aspects, rather than focussed and specific. The qualifier "legal" raised its own challenges in defining a "legal" app, since the term could potentially cover a very broad range of tools from diverse sectors and with functions ranging from document production to research, advice or self-protection.

Moreover, as our 2016 research revealed, the DTP legal app "sector" in Canada constitutes, for the most part, a fast-moving yet diffuse and uncoordinated set of small actors who are developing very different tools. This reality mirrors what is happening in the United States: in her report exploring the development of "legal tech for non-lawyers" in that country, Rebecca Sandefur observes that there are over 320 digital tools available for non-lawyer use there, with "new technologies [being] born and [dying] almost daily."[75] These tools, Sandefur continues, perform a variety of functions, including connecting individuals to lawyers, providing information, producing documents, collecting or compiling evidence, diagnosing legal problems, providing online dispute resolution or crowdfunding for bail or litigation costs.[76] Echoing our findings in the Canadian context, Sandefur concludes that in the United States, "no organization or market currently coordinates tool development. . ..[and that] [a] wide range of different kinds of actors are working to develop digital legal tools: for-profit companies, startups, non-profit organizations, and private individuals who create tools and offer them to the public through app stores like Google Play or iTunes."[77]

In both Canada and the United States, then, it seems clear that the provision of DTP legal apps is characterized by: (1) a diffuse and largely uncoordinated set of developers; (2) significant diversity in tool functionality; and (3) instability and rapid development in what is being offered to the public. On the one hand, these features of the DTP legal app sector call out for the independent development of best practices guidance. On the other hand, however, these same features pose challenges to the creation of meaningful guidance that is broadly applicable and capable of being adopted "sector-wide."

---

[74] This same challenge in defining a sector in the high-tech context of connected cars was commented on by Akalu, *supra* note 68 at 8, where he wrote: "Defining the sector or technology to establish the scope and application of a code of practice therefore represents a significant challenge."

[75] Sandefur, *supra* note 26.

[76] *Ibid*.

[77] *Ibid* at 14.

V. Access to Justice and Legal Services: The Role of Law Societies

A further challenge that arose in our project resulted from the fact that DTP legal apps intersect not only with privacy regulation and regulators but also, potentially, with legal services regulation and regulators. In Canada, fourteen provincial and territorial law societies regulate the country's roughly 125,000 lawyers.[78] Traditionally, the focus of Canadian law societies has been on ensuring that member lawyers are sufficiently competent to practice law and do not engage in misconduct by, for example, stealing from their clients or lying to the court. Since 2007, the Law Society of Ontario has been unique in Canada in that it also regulates a second set of legal professionals—paralegals—who, like lawyers, provide legal services, but on a more limited scope.[79] The law societies' mandates and powers are set out in their individual constitutive statutes. The wording of such governing legislation varies between jurisdictions but, as a general matter, it references law society authority over regulating "persons" who "practice law" or in the case of Ontario who "practice law" or "provide legal services."[80] As a corollary to this jurisdiction, there are statutory prohibitions against unauthorized persons (i.e. non-lawyers or in Ontario non-lawyers and non-paralegals) practicing law or providing legal services.[81]

Tools like DTP legal apps, that address the public's legal needs through technology, raise two interrelated issues in respect of law society jurisdiction: (1) does the function of the tool amount to *practicing law* or *providing legal services* such that it falls under law society regulatory jurisdiction; and (2) if so, does the fact that a machine is performing the function limit the law societies' jurisdiction given the statutory references to regulating *persons* who practice law or provide legal services?

With respect to the first question, DTP legal apps often provide disclaimers stipulating they are not providing "legal services" or "legal advice."[82] For users, this can be helpful information, clarifying that the service being provided by a DTP legal app is not equivalent to that provided by a licensed lawyer or paralegal (for better or for worse!). In some cases, users might also benefit from reminders that solicitor-client privilege and/or lawyer confidentiality do not apply to their communications via the app. Although most DTP legal apps are not likely to create a lawyer-client relationship such that the special

---

[78] Federation of Law Societies of Canada, "About Us" (accessed 12 December 2019), online: < https://flsc.ca/about-us/ > .

[79] Law Society of Ontario, "Paralegals" (accessed 12 December 2019), online: < https://lso.ca/public-resources/your-law-ontario-law-simplified/paralegals > .

[80] See, for example, *Law Society Act*, R.S.O. 1990, c. L.8 (Ontario): 4.1 It is a function of the Society to ensure that, (a) all persons who practise law in Ontario or provide legal services in Ontario meet standards of learning, professional competence and professional conduct that are appropriate for the legal services they provide

[81] See, e.g., *ibid* at s. 26.1.

[82] See, e.g., Bardal, *supra* note 8; Om, *supra* note 14.

confidentiality protections apply, the popularization of solicitor-client privilege through television and other media may mean that users of DTP legal apps expect that any information they share through a legal app is protected in this way. Ensuring that the public is warned against such mistaken assumptions may require some form of notification that no solicitor-client relationship is created.

Although notifications indicating that an app provides only legal information and not advice and that no solicitor-client relationship is created by using a legal app may be important pieces of information, they are not directly related to compliance with data protection law. This raises a particular challenge in the creation of a "best practices" guide for privacy and DTP legal apps. While the title of any such guide might purport to limit its scope to privacy issues, some developers could view it as a more complete type of compliance document for legal apps in relation to informing users as to how their personal information will be protected and/or used. For this reason, we recommend in our guidance the inclusion of express reminders about the nature and scope of the app's collection and use of private information.

Notwithstanding any disclaimers to the contrary, when it comes to DTP legal apps, there is an objective question as to whether they are in fact providing "legal services" such that the jurisdiction of the law societies is engaged. While a developer of a DTP legal app may well announce that their app does not provide legal advice or legal services, this does not translate, in itself, to a concrete reality (i.e. that the app is not performing these functions). However, answering the objective question of whether a DTP legal app is providing legal advice or legal services, as these terms are statutorily defined, is not a straight-forward matter. One common approach is to draw a distinction between "legal information" and "legal advice."[83] While the provision of legal advice is restricted to lawyers and Ontario paralegals, anyone can provide "legal information." The legislative and regulatory distinction has historically created some challenges. As Jennifer Bond, David Wiseman and Emily Bates have observed,

> While these two concepts can be clearly distinguished and applied in some circumstances, many projects are not easily categorized according to this dichotomy-which is simultaneously strictly applied and poorly defined. These complexities have particular relevance in the context of the access to justice crisis because of the emphasis on finding innovative ways to provide meaningful legal assistance to mitigate deficits, often via legal support service models that assist with the consumption of legal information.[84]

---

[83] See, e.g., Canadian Forum on Civil Justice, "'Legal Advice' vs. 'Legal Information': Clearing Up the Murky Water" (26 September 2017), online: <http://www.slaw.ca/2017/09/26/legal-advice-vs-legal-information-clearing-up-the-murky-water/>.

[84] Jennifer Bond, David Wiseman & Emily Bates, "The Cost of Uncertainty: Navigating the Boundary Between Legal Information and Legal Services in the Access to Justice Sector" (2016) 25 J.L. & Soc. Pol'y 1.

In the United States, some of the most prominent battles over the question of what constitutes the practice of law (such that only lawyers can engage in it) have involved the online provision of legal documents to the public through companies like LegalZoom, which in 2001 launched ten web-based products that focused on estate planning, business formation, and intellectual property protection.[85] In large part, LegalZoom's business involves providing online forms directly to the public, although, after nearly a decade of operation, LegalZoom created an "independent attorney network" through which individuals can also receive personalized legal advice.[86] Since LegalZoom's launch, its operations have been challenged as constituting the unauthorized practice of law through a variety of means including investigations, lawsuits, cease-and-desist letters and bar ethics opinions.[87] LegalZoom's ability to prevail against these challenges has been mixed.[88] In some instances, courts have ruled in favour of LegalZoom, finding that its practices do not constitute the unauthorized practice of law while, in other cases, courts have ruled against LegalZoom on this legal question.[89] LegalZoom has also chosen to pay money to settle cases and has entered into settlements that have required it to change its business practices.[90] To be sure, overall, LegalZoom has clearly been able to run and maintain a very successful business in the face of such challenges: in 2015, the company reached 3.6 million consumers[91] and in 2018, it received a $2 billion valuation.[92] The experience of LegalZoom in the United States nonetheless

---

85 LegalZoom, "About Us" (accessed 12 December 2019), online: < https://www.legalzoom.com/about-us > [LegalZoom].

86 For further background on LegalZoom, see *ibid*; Benjamin H. Barton, *Glass Half Full: The Decline And Rebirth of The Legal Profession* (New York: Oxford University Press, 2015) at 88-97 [Barton].

87 For a summary of some of these challenges, see Cody Blades, "Crying Over Spilt Milk: Why the Legal Community is Ethically Obligated to Ensure LegalZoom's Survival in the Legal Services Marketplace," (2015) 38 Hamline L. Rev. 31 (reporting, "[i]n 2010, LegalZoom faced legal challenges from Missouri residents and the Washington State Attorney General's office. In 2011, lawyers from the DeKalb County Bar Association of Alabama sued LegalZoom, asking the court to enjoin LegalZoom from continuing business In 2012, LegalZoom's services were challenged by the North Carolina State Bar and a resident of Ohio. Finally, in 2013, class actions against LegalZoom were filed in both Texas and Arkansas. LegalZoom reported a $5.4 million loss related to the company's legal settlements on their initial public offering.").

88 For further discussion see Barton, *supra* note 85; Susan Saab Fortney, "Online Legal Document Providers and the Public Interest: Using a Certification Approach to Balance Access to Justice and Public Protection" (2019) 72 Oklahoma L. Rev. 91 at 97-104 [Fortney].

89 *Ibid*.

90 *Ibid*.

91 LegalZoom, *supra* note 85.

92 Gerrit De Vynck, "LegalZoom Gains $2 Billion Valuation in Funding Round" *Bloomberg* (31 Juy 2018), online: https://www.bloomberg.com/news/articles/2018-07-31/legalzoom-gains-2-billion-valuation-in-latest-funding-round.

reflects the fact that the parameters of what constitutes legal practice when it comes to DTP legal apps has been highly contested ground. Additionally, as several American commentators have noted, LegalZoom's ability to weather numerous challenges is likely due in no small part to its size, both in terms of the financial resources that it can bring to bear to defend itself as well as its relative prevalence in the market-place.[93] As noted above, current providers of DTP legal apps in Canada tend to be relatively small and would presumably be much more fiscally constrained in fighting similar challenges.

Our research has not revealed any publicly reported investigations or proceedings against DTP legal app providers in Canada for unauthorized practice. As part of our 2016 research on legal apps, we surveyed Canadian law societies and, at that time, the law societies indicated that they had not received any complaints about legal apps.[94] At the same time, however, multiple law societies did express concerns about the potential harm that unregulated legal apps could cause to the public, particularly if such apps are providing legal services.[95] For some of the app developers that we consulted as part of this project, the prospect of law society regulation was a source of anxiety. Indeed, DTP legal app developers conveyed to us that, in some cases, fear of after-the-fact law society regulation was a significant disincentive to innovation. We were also told that, in at least one case, the law society conducted an investigation in relation to a DTP legal app. This investigation, we were told, was conducted privately and was not reported more broadly to the public. We do not know if there are any additional non-reported investigations of DTP legal app providers.

In general, a significant amount of the investigatory and disciplinary work of Canadian law societies occurs privately and is not subject to freedom of information statutes.[96] As a result, information about the exact nature and scope of regulators' engagement with DTP legal apps is not readily available. It is safe to say, however, that uncertainty and confusion currently exists in the DTP legal apps sector as to the proper role and intentions of law societies in regulating DTP legal apps. At least some stakeholders in the DTP legal apps sector believe that this possibility is creating a chilling effect on innovation. Although large actors like LegalZoom may be willing to take on potential regulatory investigations and legal proceedings as acceptable risks of doing business, the DTP legal app developers that we talked to expressed significant caution and concern. Whether larger providers with potentially more appetite for risk will begin to provide DTP legal apps in Canada remains to be seen—the Canadian market is much smaller

---

93 See, e.g. Barton, *supra* note 85 and Fortney, *supra* note 87.

94 McGill et al., SSHRC, *supra* note 20 at 21.

95 *Ibid.*

96 For more information about the lack of transparency in law society investigatory and discipline processes, see Amy Salyzyn, "Law Society Complaints: What We Don't Know and Why This Is a Problem" *Slaw.ca* (10 June 2015), online: < http://www.slaw.ca/2015/06/10/law-society-complaints-what-we-dont-know-and-why-this-is-a-problem/ > .

than the United States' and the fact that legal needs often require jurisdiction-specific solutions shrinks the market for many products further.

The uncertainty about when DTP legal apps are providing legal services, and thus potentially fall under law society jurisdiction, is not something that we address in our guidance. In addition to being outside our goal of providing privacy best practices, the vague and variable legal information/legal services dichotomy means that, in significant ways, the answer to when a given DTP legal app or class of apps will attract the regulatory attention of law societies is only answerable by the law societies themselves. There is no clear test or precedent on which to rely. To date, no Canadian law societies have provided any proactive public guidance on this important question, and there remains the matter of whether more guidance should in fact be provided, and if so, what its likely impacts might be. On the one hand, guidance could help clarify when developers need to be concerned with law society jurisdiction. On the other hand, some developers cautioned that articulating a bright line between legal information and legal advice could be potentially stifling to innovation and motivate more enforcement activity. Whether law societies should issue such guidance raises foundational questions regarding the exact nature of their jurisdiction over the provision of legal advice generally and DTP legal apps more specifically. To the extent that a DTP legal app could be classified as providing legal advice or legal services, some have noted that an additional question arises about whether and how law societies have jurisdiction over machines (as opposed to persons) providing legal advice given that statutory grants of law society jurisdiction refer explicitly to persons.[97]

Notably, questions regarding whether and how lawyer regulators might govern the delivery of DTP legal apps are being discussed in other jurisdictions. For example, in March 2019, the California State Bar's Task Force on Access Through Innovation of Legal Services—Subcommittee on Unauthorized Practice of Law analyzed a proposal that "legal advice devices" be directly regulated, as opposed to only regulating those providing the devices, in a manner akin to the U.S. Food and Drug Administration's regulation of "medical devices."[98] In July 2019, this Task Force released sixteen "concept options for possible regulatory changes" for public input, which includes proposals to add an exception to the state's prohibition against the unauthorized practice of law to permit "technology-driven legal services delivery systems" to engage in the practice of law on the condition that they are subject to a certification,

---

[97] For further discussion of this question, see Nate Russell, "Who Dunnit? Artificial Intelligence and Unauthorized Practice" *Slaw.ca* (8 November 2017), online: < http://www.slaw.ca/2017/11/08/who-dunnit-artificial-intelligence-and-unauthorized-practiced/ > .

[98] Wendy Chang, *Provider Regulation vs. "Legal Advice Device" Regulation* (Memorandum submitted to Task Force on Access Through Innovation of Legal Services—Subcommittee on Unauthorized Practice of Law and Artificial Intelligence, 26 March 2019), online: < https://board.calbar.ca.gov/Agenda.aspx?id = 15170&tid = 0&show = 100021302#10029144 > .

registration or approval process and that such systems be subject to "adequate ethical standards that regulate both the provider and the technology itself."[99]

Other American states have also been considering regulatory reform. In Tennessee, proposed legislation would deem the publisher of a website that offers interactive legal forms directly to consumers to be engaged in the practice of law, unless certain statutory requirements are fulfilled (including, for example, having a licensed attorney review each form first).[100] In Washington, the State Bar Association is currently consulting on proposed amendments to that state's definition of the "practice of law" to permit "online self-representation legal service providers" which includes a consideration of what restrictions and other regulatory requirements should come along with these restrictions.[101] In Utah, a taskforce has also recently recommended relaxing the definition of the unauthorized practice of law to allow for more innovative legal service delivery.[102] It has also proposed a new regulatory structure which would include a "regulatory sandbox" model in order to "permit innovation to happen in designated areas while addressing risk and generating data to inform the regulatory process."[103] These recommendations have now been unanimously approved by the Utah Supreme Court, which has authority over lawyer regulation in that state.[104]

In Canada, the Law Society of Ontario has established a Technology Taskforce and the Law Society of British Columbia has created a Futures Taskforce each with a mandate to study the influence of technology on the delivery of legal services and potential regulatory responses.[105] New approaches

---

[99] The State Bar of California, "Options for Regulatory Reforms to Promote Access to Justice" (accessed 12 December 2019), online: < http://www.calbar.ca.gov/About-Us/Our-Mission/Protecting-the-Public/Public-Comment/Public-Comment-Archives/2019-Public-Comment/Options-for-Regulatory-Reforms-to-Promote-Access-to-Justice > .

[100] Richard Granat, "Tennessee Plans to Regulate Online Legal Software Publishers" (24 February 2019), online: < https://www.richardgranat.com/single-post/2019/02/22/Tennessee-Plans-to-Regulate-Online-Legal-Software-Publishers > . The Law Society of Ontario Technology Task Force issued its first report in November, 2019: Will Morrison, Technology Task Force, Update Report (29 November 2019), online: < https://lawsocietyontario.azureedge.net/media/lso/media/about/convocation/2019/convocation-november-2019-technologytaskforce-report.pdf > .

[101] Washington Courts, "GR 24 - Changes to GR 24 Definition of Practice of Law" (accessed 12 December 2019), online: *https://www.courts.wa.gov/court_rules/?fa=court_rules.proposedRuleDisplay&ruleId=2712* > .

[102] The Utah Work Group on Regulatory Reform, "Narrowing the Access-to-Justice Gap by Reimaging Regulation" (August 2019), online: < https://www.utahbar.org/wp-content/uploads/2019/08/FINAL-Task-Force-Report.pdf > .

[103] *Ibid.*

[104] Bob Ambrogi, "Utah Supreme Court Votes to Approve Pilot Allowing Non-Traditional Legal Services" *LawSitesBlog.Com* (29 August 2019), online: < https://www.lawsitesblog.com/2019/08/utah-supreme-court-votes-to-approve-pilot-allowing-non-traditional-legal-services.html > .

to regulating DTP legal apps may be forthcoming in Canada, but they are not here yet.

In the absence of a clear regulatory mandate over DTP legal apps, it is interesting to think about a suggestion made by some of the developers we consulted: law societies could establish a method of voluntary certification of compliance with a set of standards, like a trust mark, or audits, for example. Again, in Canada, many DTP legal app providers are individuals or small teams, not large corporations with in-house legal departments. For these developers, compliance with privacy and other norms is viewed largely as a burden. Some developers told us that even compliance with best practices guidance would be cumbersome if some aspects are unclear, or if the relevance of the guidance depends on a certain factual matrix that may be difficult to interpret or apply. We heard from developers that if they are going to invest the effort in compliance, they want to have some form of public recognition that they could share with their users—in the form of a trust mark or certification.[106]

This model could be used both to reassure those providing the app that they have met required standards, and to inform the public that they app they are using has been vetted and approved. It is not clear what entity or body is best placed to provide such certification. If DTP legal apps are designed to increase access to justice, then an assessment that goes beyond privacy compliance and includes issues related to access to justice goals and the law might best come from law societies or from an entity charged by law societies with performing such assessments, rather than privacy regulators. This would also avoid the commercial/non-commercial barrier to the application of PIPEDA. However, if excluding privacy regulators would lead to law society certification of an app that is not compliant with data protection law, this would be problematic. A foundational question similar to those raised above is also at play: does this kind of certification function properly fall within the law societies' current regulatory mandates, which centre on ensuring the competent and ethical practice of law? Some DTP legal apps may clearly fall within the definition of "the practice of law" but others will clearly be excluded. Moreover, a significant subset of DTP legal apps may be hard to classify given, as discussed above, the murky boundary between what constitutes the "mere" provision of legal information as opposed to the provision of legal services such that Canadian law societies have regulatory jurisdiction. There are also practical questions as to whether Canadian law societies, which vary significantly in size and resources, would all have the

[105] For more information, see Law Society of British Columbia, "Mandates Established for Futures Task Force and Annual Fee Review Working Group" (12 March 2019), online: <https://www.lawsociety.bc.ca/about-us/news-and-publications/news/2019/mandates-established-for-futures-task-force-and-an/>; Law Society of Ontario, "Committees" (accessed 12 December 2019), online: <https://lso.ca/about-lso/governance/committees?lang=en-ca>.

[106] For a discussion of certification and trust marks, see, e.g., Amanda Craig, "Federated Identity Management and the NSTIC: Co-Managing Information Privacy" (2014) U. Ill. J.L. Tech. & Pol'y 177.

necessary expertise and resources to create and maintain certification processes for DTP apps.

If law societies are not the best place for certification, perhaps the profession's advocacy bodies such as the Canadian Bar Association ("CBA") and its provincial counterparts hold promise. Here, too, there is concern about a mismatch with mandate. Although the CBA includes as part of its stated mission to "improve and promote access to justice," at its core, the role of the CBA is to advocate for its members' (i.e. lawyers and paralegals) professional and commercial interests.[107] To the extent that DTP legal apps can be seen as displacing the need for lawyers' services, they may be seen as contrary to CBA members' interests, at least narrowly understood.

Susan Fortney, an American law professor, suggests another alternative: a private certification regime that "could both benefit online document providers and advance public protection."[108] In advocating for such an approach, Professor Fortney notes that a private regulatory regime could help overcome some of the issues with law society regulation, including lack of resources and jurisdictional issues, as well as help to reduce developer concerns that they will be subject to after-the-fact regulation.[109] In terms of the administration of such a certification regime, she suggests, "a non-profit group [like the International Bar Association (IBA) and the Conference of Legal Regulators (ICLR)] could spearhead a process to examine different approaches to certification."[110]

In our opinion, the private certification regime approach is worth considering in relation to DTP legal apps. We do acknowledge, however, that additional challenges are likely to arise in relation to Canada's DTP legal app sector, which is distinct in many ways from the automated legal document sector in the United States studied by Professor Fortney. The latter contains multiple large and well-resourced actors who produce tools with significant similarities in function. As noted above, the Canadian DTP legal apps "sector" constitutes, for the most part, a fast-moving but diffuse and uncoordinated set of small actors who are developing in some cases very different types of tools to respond to diverse access to justice needs. Moreover, in the case of DTP legal apps, the question of how a private certification regime would be funded is live; if the cost is put on developers, this could create a new disincentive to the development of digital tools that advance the public interest. Other options for funding private certification include lawyers, taxpayers or app users, but each of these raises its own challenges.

---

[107] Canadian Bar Association, "Mission and Vision" (accessed 12 December 2019), online: < http://www.cba.org/Who-We-Are/About-us/Mission-and-Vision. >

[108] Forney, *supra* note 88.

[109] *Ibid.*

[110] *Ibid.*

VI. A Sectoral Code versus a Best Practices Guide

As noted earlier, the goal of our OPC-funded project was to produce a kind of "sectoral code" for DTP legal apps. This was in line with the desire of the OPC to explore the potential of sectoral codes as a means of providing more tailored guidance for PIPEDA compliance. However, the challenge of defining the boundaries of legal apps, combined with the fact that so many of the PIPEDA compliance issues raised by legal apps are inherent in apps generally, made a formal code an awkward fit. If we focussed too broadly on issues raised by apps generally, we risked replicating work that had already been done by the OPC on providing privacy guidance to app developers generally. On the other hand, if we focussed narrowly on the "industry" context of these apps insofar as they address legal needs, the specific privacy issues raised often overlapped with questions related to the competence of provincial and territorial law societies, as discussed above.

A further issue is that the not-for-profit and access to justice considerations that drive the development of many legal apps create challenges within the governing legal frameworks. As noted above, PIPEDA applies only to the collection, use or disclosure of personal information in the course of commercial activity.[111] Free legal apps offered as a public service do not fall within its scope. This might mean that PIPEDA compliance is not required for many DTP legal apps. Further, while PIPEDA applies to inter-provincial and cross-border commercial activity (and thus generally applies to apps in the commercial sector), some legal apps that are designed to assist individuals with legal matters falling within areas of provincial jurisdiction are intended only for intra-provincial use. PIPEDA will still apply to intra-provincial commercial activity in provinces that do not have substantially similar legislation applicable to the private sector. However, in provinces that do have such legislation, such as Alberta, British Columbia and Quebec, the private sector data protection laws of those provinces would apply. While a general privacy code of practice for PIPEDA compliance would provide useful information applicable in those other jurisdictions as well, there might be matters of differing importance, and certainly different information might need to be provided about which regulator to turn to for further guidance. To complicate things further, in British Columbia, the private sector data protection law applies to the non-commercial activities of non-profits.[112] Thus, although the application of data protection laws to non-profit legal app provision remains a key gap in most Canadian provinces and territories, in some provinces compliance with privacy laws is required even if an app is not commercial.

Not only is the complicated web of privacy laws in Canada difficult to untangle in a simple guidance document intended for DTP legal app developers, the fact that such explanations are necessary suggests that a single sectoral code

---

[111] PIPEDA, *supra* note 1, s. 4(1)(a).

[112] B.C. PIPA, *supra* note 32 at s. 1 definition of "organization" and s. 3.

approach is inappropriate in areas where the applicable law is not clear. It is one thing to develop a code for a federally regulated sector of the economy—and one that is entirely commercial—such as banking. It is quite another to develop one for a sector that is occupied by non-profit as well as for-profit actors, some of whom operate intra-provincially and some of whom operate on a national basis. While a general set of best practices can still be useful, it is not quite a sectoral code. For these reasons, in the end we chose to call the document that we developed a best practices guide.

A further issue with the "sectoral code" approach is that we ourselves are not part of the sector to be regulated. Industry associations that represent the companies operating in the sector that will be governed by the code develop most sectoral codes.[113] These organizations have the resources and capacity to co-ordinate the development of a code; through the participation of their membership they can achieve representation on the committee charged with drafting the code, and they have internal mechanisms for approving and adopting the code. Such practices give the code legitimacy within the sector bound by the code. The collaborative process, even with a voluntary code, may create a useful kind of "peer pressure" to encourage compliance with the code in order to maintain good standing within the association. Although we were encouraged to consult widely in the development of our code and we did reach out to developers both at the outset and in reviewing our draft codes, a code imposed from outside the legal app sector simply would not have the normative weight of a sectoral code developed by an industry association.

Not only are we not industry representatives, we are not regulators. We interrogated the relationship between providing tangible documents and producing regulation. Since we are not regulators, it is not our role to be prescriptive. In addition, because the actors in the field of legal apps are so diverse, it would be difficult to anticipate all situations or provide uniformly applicable advice. These concerns arose again when we considered the dissemination of our work. While we believe the best practices document we developed is a good one, we struggled with whether we should host it on a website. Many developers had suggested it would be useful in a layered digital format, and we see merits in this approach. However, we do not have the resources necessary to maintain and update the document (or website) indefinitely, and given that the technology changes rapidly, and that reform of PIPEDA seems to be an at least somewhat likely prospect,[114] we are concerned about creating a digital document that could not be kept up to date.

---

[113] See the examples referenced in footnotes 70, 71, and 72.

[114] Innovation, Science and Economic Development, "Strengthening Privacy for the Digital Age: Proposals to Modernize the Personal Information Protection and Electronic Documents Act" (May 21, 2019), online: < https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html > .

CONCLUSION

In this article, we have reflected on some of the challenges we faced and the lessons we learned in working on a privacy best practices guidance for the development of DTP legal apps.

One of the reasons for defining DTP legal apps as a distinct category of apps was precisely the intersection between legal services as part of a regulated profession, legal information as an aspect of access to justice, and access to justice as a combination of access to professional legal advice and general legal information. DTP legal apps may tread a difficult line in terms of both their relationship to regulated legal services and their goal of making legal information more readily accessible—including to those who may not be able to afford professional legal services. While privacy laws might apply on both sides of the line, the first category of DTP legal apps may also be impacted by professional regulations, while the second category would not. This dual nature of DTP legal apps complicated our project. Not only was it difficult to draw the line in some cases between regulated legal services and the provision of legal information, we found that law societies themselves are not always certain of how to address DTP legal apps as an aspect of legal services. Ultimately, Canadian law societies will be forced to provide more clarity regarding how they understand their jurisdictional mandates to interact with DTP legal apps. To be sure, this sort of line drawing exercise carries risks of regulatory overreach both from a definitional standpoint (i.e. the risk of too many tools being classified as within the law societies' jurisdiction) and an enforcement standpoint (i.e. the risk that a more precise definition of what tools are within the law societies' jurisdiction will motivate more complaints and investigations by law societies than currently take place). Even with a clearer definition of which DTP legal apps are the law societies' concern, there remains the question of those DTP legal apps that still fall outside the law societies' regulatory reach.

With respect to privacy risks, the OPC and other privacy regulators are charged with ensuring compliance with a set of standards (to the extent that such apps are "commercial"). What about non-commercial apps and risks that go beyond privacy? Additional sets of best practices may be useful, but DTP legal app developers need to be motivated to review and use them. A voluntary certification may be the best answer to this problem, but there are significant issues with respect to management and funding.

Another lesson learned is that digital technologies create recurring issues across a broad range of sectors, making sectoral codes less useful, perhaps, than thematic ones (i.e. how to deal with specific technologies or commercialization practices). While there were some context-specific issues raised by DTP legal apps, many of the issues are common to apps in general. This does not mean there is no merit in addressing the particular needs of legal app developers in a guidance document, but it is something far different from a sectoral code.

These complexities do not, in our view, detract from the merits of the exercise we engaged in or the value of the document we have produced. Our project

brought key players together, fostered dialogue, and generated context-specific knowledge. While not a sectoral code in any true sense, our best practices guide, we believe, contains useful information arranged in an accessible manner and is designed to address many of the issues specific to the legal apps context.

The complexities in turn have enriched our understanding of DTP legal app development, privacy and the relationships between legal apps and access to justice seen through the lens of privacy protection. We hope that the lessons learned can add to further discussions about how best to develop sector-specific privacy guidance, as well as how to provide oversight of legal service, legal information, and access to justice technology in the public interest.

APPENDIX

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 at (<https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/>)

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 at https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/. 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. 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. ***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.

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—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 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 3203601), 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."[115] 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.[116]

---

[115] Lisa M. Austin et al., "Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project" (2018), online: < https://ssrn.com/abstract = 3203601 > or < http://dx.doi.org/10.2139/ssrn.3203601 > .

Legal app developers who are using ad libraries should consult the OPC's guidance (https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/) 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.

---

[116] *Ibid* at 25.

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 (https://www.canlii.org/en/ca/scc/doc/1989/1989canlii20/1989canlii20.html) 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 (https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/) 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 (https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/) 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 (https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/) 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 (https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/02_05_d_56_tips2/) 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 (https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/gd_app_201210/) 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 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 (https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/) 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 (https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/) 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 (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/) 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

Lisa M. Austin et al., "Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project" (2018), online: <https://ssrn.com/abstract=3203601> or <http://dx.doi.org/10.2139/ssrn.3203601>.

Edmonton Journal v. Alberta (Attorney General), 1989 CarswellAlta 198, [1989] 2 S.C.R. 1326 (S.C.C.).

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

Office of the Privacy Commissioner of Canada, "Guidelines on Obtaining Meaningful Consent" (May 2018), online: < 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), online: https://www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/gl_ba_1112/ > .

Office of the Privacy Commissioner of Canada, "Personal Information," PIPEDA Interpretation Bulletin (11 October 2013), online: < 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, "PIPEDA Fair Information Principle 7—Safeguards" (January 8, 2018), online: 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/ > .

Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principles" (May 2019), online: < 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, "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps" (October 2012), online: < 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, "Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency" (November 2018), online: < https://www.priv.gc.ca/en/privacy-topics/privacy-policies/02_05_d_56_tips2/ > .

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.