
GOING MOBILE: LEGAL CONSIDERATIONS FOR MOBILE APP DEVELOPMENT

*By Colin J. Thurston **

A. INTRODUCTION

Canadian charities and not-for-profit organizations have by now fully realized that developing a strong online presence, including a modern and attractive website, is a crucial factor in an organization's continued success. Moreover, the internet has presented a cost-effective opportunity that has been embraced for advertising and promoting an organization and its goals to a global audience. More recently, many charities and not-for-profits have begun to venture into the world of mobile applications ("apps") for smartphone and tablet devices. This now well-established online marketplace allows for-profit enterprises as well as charities and not-for-profits to offer digital goods and services to millions of Canadians through their mobile devices at any time and in any place. As more charities and not-for-profits begin taking advantage of this new and innovative platform for connecting with the public, there are a number of legal and practical considerations which need to be kept in mind. This *Charity Law Bulletin* outlines some of these considerations in relation to information security, privacy and the protection of an organization's intellectual property, which matters will be relevant to the development and operation of virtually any new mobile application.

* Colin J. Thurston, B.A., J.D. is an associate of Carters Professional Corporation and a registered trade-mark agent with the Canadian Intellectual Property Office. Colin practices at our Orangeville office in the areas of intellectual property, privacy and information technology.

B. INFORMATION SECURITY AND PRIVACY

Much like the organization's existing website, a mobile application will almost certainly involve the collection of at least some user information, and in doing so will raise questions regarding what the organization is doing with the information it collects, and what steps it has taken to comply with its obligations under federal and provincial privacy laws. Organizations will already be familiar with federal privacy legislation¹ ("PIPEDA") and the practical need for online privacy statements and internal privacy policies. Federal and provincial privacy laws require, among other things, that where personal information about an individual is collected, used or disclosed by an organization, consent must first be obtained from the individual to such collection, use or disclosure. Additionally, personal information is required to be stored securely, remain accessible by the individual upon request and retained only as long as necessary to fulfill the purposes for which it was collected.

Federal privacy legislation applies in most provinces, except for Quebec, Alberta and British Columbia, which have their own private sector privacy laws.² While federal privacy legislation applies with respect to information collected in relation to "commercial activity", certain provincial legislation applies regardless of whether activities are of a commercial nature. However, it is important to note that even under the federal legislation what is considered to be "commercial activity" can include the activities of a charity or not-for-profit, and the fact that an app is not generating revenue does not mean that PIPEDA does not apply.³ Certain definitions in PIPEDA specifically mention donor lists, making some activities of charities explicitly subject to the act.⁴ Charities and not-for-profits should therefore exercise due diligence in extending their efforts to comply with privacy legislation to any new mobile applications, in addition to their existing privacy compliance efforts, such as in relation to the organization's website.

As a mobile app will often be designed to achieve a different purpose than that of an organization's website, there are often differences in the type of personal information that an app may collect. For example, while an organization's website may focus primarily on providing information and resources to donors and the public, a mobile app for a charity or not-for-profit might be developed for the purpose of tracking a donor's participation in a fundraising campaign, for allowing members to "check-in" to common locations of

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

² McIsaac et al., *The Law of Privacy in Canada*, looseleaf (Toronto, ON: Carswell, 2000) at 4.1.5.

³ Office of the Privacy Commissioner of Canada, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* (October 2012), available online at: http://www.priv.gc.ca/information/pub/gd_app_201210_e.asp.

⁴ *Supra*, note 1, s. 2 (1).

interest, or for allowing the app's user to post relevant updates to social media accounts. As most mobile devices include digital cameras, many apps support photo-sharing, including location tagging and identification of photographed individuals. Advertisers and advertisements will often play a role in making mobile apps available for free, and some developers' apps may seek access to user data for advertising or other purposes. In this regard, charities and not-for-profits need to keep in mind that any information which may be used to identify an individual, or which can be connected to an individual user, may be considered "personal information" and subject to privacy laws. This can include names and contact information, but can also include photographs, location data and other collected information.

In response to the proliferation of mobile apps now available, a collaborative guidance document was released in October, 2012 by the privacy commissioners of Canada, Alberta and British Columbia, titled *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*.⁵ Among other things, the document confirms the following general principles which should be taken into account when developing mobile applications:

- **The organization is ultimately accountable.** Even though an organization will typically contract with third-party developers for the development and operation of a new app, it is ultimately up to the organization to ensure that users' personal information will be handled in accordance with the organization's privacy policies and in compliance with federal and provincial privacy laws.
- **App development practices are drawing attention from governments and consumers.** The best practice is to be open and transparent about the organization's privacy practices, including initial and ongoing disclosure of personal information handling practices and any changes to those practices, including changes to the organization's privacy policy.
- **Information collection should be limited.** Only information that is necessary for the functioning of the app should be collected. In general, if the organization cannot explain how a piece of information it collects is related to the functioning of the app, then this information should probably not be collected.

⁵ *Supra*, note 3.

- **The reasons for collecting information should be identified.** An organization should never collect information without a specific purpose, or because it believes the information may become useful in the future. Any current or proposed use of personal information should be disclosed at the time the information is collected.
- **Information must be securely stored.** Data and privacy breaches can result in fines, lawsuits and other financial consequences to an organization, and also make for popular news topics which can lead to much negative publicity. If information is stored with a third-party, the responsibility for ensuring that the information is secure will ultimately rest with the organization.

The guidance document also provides helpful information for developing privacy notices for mobile devices, which devices are limited by their screen size compared to a standard desktop or laptop computer. Strategies for using graphics and abbreviated privacy statements are discussed. Of particular importance, the guidance document notes that some developers and other companies now offer privacy policy template language generators for mobile apps and other applications. Organizations need to exercise caution when accepting or using such policy wording, as the organization will be held accountable for its content. Legal counsel should be consulted to ensure that the policy statement meets the organization's objectives as well as its obligations under Canada's privacy laws.

In considering the development of a mobile app, a charity or not-for-profit will need to apply the same principles in relation to protection of personal information as it does in relation to its website and other activities, though heightened awareness is urged in relation to mobile apps, which may collect novel forms of personal information and which may be more vulnerable to breaches of security and privacy. As with any other change affecting an organization's collection or handling of personal information, the organization's privacy statements, policies and internal practices will need to be reviewed and updated to ensure continued compliance. Additionally, when contracting with third parties for IT services it should never be assumed that the contracts are non-negotiable, and legal counsel should be involved in negotiating and reviewing agreements with app developers and other contractors, including data storage and cloud service providers.

C. PROTECTING THE ORGANIZATION'S INTELLECTUAL PROPERTY

In addition to protecting the personal information of the app's users, the organization also has an interest in protecting the content and design of the app itself. Similar to other written or electronic publications or resources of the organization, the app is a valuable product comprised of proprietary information and intellectual property which the organization will want to control and protect. In this regard, the organization will no doubt be granted certain rights regarding the mobile application under its contract with the developer, though the granting of ownership and/or access rights may vary depending on the contract. Determining the respective rights of the organization and the contracted developers and service providers will need to be considered in the early stages of planning a new app development, as opposed to at some later time after a dispute or problem has arisen. Some important points to keep in mind are discussed below:

- **Copyright Ownership.** A mobile app, like a website or computer program, is at its most basic level a written computer code. Such computer code (often referred to as "source code") can be the subject of copyright protection. Copyright is an automatic right which vests in the *creator* of a copyrightable work, and the copyright owner has the right to prevent others from copying or reproducing the work in any form. Importantly, this copyright will *not* automatically be transferred to the organization merely because it has paid a contractor for the work. The rights to the work must be assigned to the organization in writing. This means that the contract with the developer will need to clearly set out the eventual ownership rights with respect to the app that the developer is being hired to create. Additionally, the organization should obtain a representation that the creator will waive any moral rights to the work, which might otherwise prevent the organization from later modifying the source code. The contract with the app developer should be reviewed by legal counsel.
- **Ownership of Mobile App Data.** This point is related to the privacy issues discussed above regarding security and handling of personal information. Also relevant in this regard is the determination of who will own any data that is created and/or collected through the mobile app, including statistical data and information of a non-personal nature. This needs to be addressed under the contract with the app developer, and also with any third-party company which stores data either in-house or as a cloud data service. The ability to retrieve and access data during the term of

the contract is an important consideration (particularly if the app produces statistical data for research purposes), as is the right of a service provider to delete data in its possession either during the agreement, upon termination of the agreement or some time thereafter. This should all be addressed up front in the contract with the service provider.

- **Trade-mark Protection.** In all likelihood, the app will display the organization's existing trade-marks including the name of the organization, its logo, taglines or program names. If the trade-marks are not registered so as to ensure Canada-wide usage rights, then it is recommended that registration be pursued as soon as possible, as the app will likely be available throughout the country. Additionally, even if the trade-marks are registered, the existing registrations may not extend rights to the new use of the trade-marks (*i.e.*, in association with a mobile application), and therefore existing registrations may need to be expanded to protect the new use. It is also possible that the new application will involve the development of one or more new trade-marks. For example, the name of the app or the app's home screen icon may be suitable for protection as new trade-marks. It is recommended that organizations conduct due diligence searches with the assistance of legal counsel and apply for registration of such trade-marks before they are used. Additionally, trade-mark rights are granted on a country-by-country basis and so if the app will be available in countries other than Canada, searching and registration should be undertaken in those countries as well.

These and other matters should be discussed with legal counsel at the early stages of developing a new app, and it is therefore recommended that legal counsel be engaged early in the process.

D. CONCLUDING COMMENTS

As charities and not-for-profits continue to take advantage of the mobile app as a new platform for delivery of online communication and services they will increasingly need to familiarize themselves with the legal and regulatory requirements affecting new technologies. Privacy compliance in particular is an area of increasing application and complexity. The application of federal and provincial privacy legislation to the activities of charities and not-for-profits will continue to be of significance as these organizations adopt the same communications technologies which the for-profit sector has already widely used to its substantial benefit. As already mentioned above, however, this use of technology has already attracted the attention of

authorities and governments, and organizations' information handling practices will continue to come under scrutiny. In that regard, efforts to ensure compliance now will be rewarded going forward, as organizations are forced to continually adapt to the changing legal and regulatory environment of current and future mobile technologies and other innovative modes of online communication which charities and not-for-profits will want to use to their full advantage.



Carters Professional Corporation / Société professionnelle Carters
Barristers · Solicitors · Trade-mark Agents / Avocats et agents de marques de commerce
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca

Ottawa · Toronto
Mississauga · Orangeville
Toll Free: 1-877-942-0001

DISCLAIMER: This is a summary of current legal issues provided as an information service by Carters Professional Corporation. It is current only as of the date of the summary and does not reflect subsequent changes in the law. The summary is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.

© 2013 Carters Professional Corporation