CROSS-BORDER PRIVACY ISSUES

U. Shen Goh
Carters Professional Corporation
Toronto

Canadian Privacy Legislation Requires Consent; U.S. Anti-Terrorism Legislation Takes Away Consent*

Introduction

Statistics Canada indicates that there are more than 161,000 charitable and non-profit organizations currently operating in Canada.[1] This includes hospitals, universities, private schools, food banks, environmental groups, day-care centres, sports clubs, places of worship, social justice groups, groups that raise funds and awareness for various diseases, etc. Collectively, the 161,000 charitable and non-profit organizations have revenues totalling $112 billion,[2] $8 billion of which come from individual donations.[3] These organizations also draw upon two billion volunteer hours and 139 million memberships.[4]

The question, however, is how do these organizations raise the funds and find the volunteers that are fundamental to their organizations' existence? Before any organization can call or mail an individual to solicit funds or volunteers, the organization will need to have access to the individual's personal contact information. This article explains how Canadian privacy legislation requires consent to do so, how such consent may be lost through U.S. anti-terrorism legislation, and what Canadian charitable and non-profit organizations can do to protect their donors, supporters, members, employees, volunteers and themselves.

Canadian Privacy Legislation

The *Personal Information Protection and Electronic Documents Act*[5] ("PIPEDA") is the federal legislation in Canada that applies to every organization that collects, uses or discloses personal information in the course of commercial activities. In addition, Alberta, British Columbia and Québec have provincial legislation substantially similar to PIPEDA that applies to every organization that collects, uses and discloses personal information, regardless of whether or not it is for commercial purposes. Furthermore, Ontario has provincial legislation regulating the collection, use and disclosure of personal health information, especially in relation to fundraising activities.

Each of the legislation cited above has different standards for privacy protection and consent to use an individual's personal information. Depending on the location(s) and activities of the specific charitable or non-profit organization, it is possible for different organizations to be subject to one or more of the legislation cited above. Speaking generally, however, it is clear that all the Canadian privacy legislation requires consent for the collection, use and disclosure of personal information in the following circumstances:

PIPEDA

PIPEDA requires consent for the collection, use or disclosure of personal information in the course of commercial activities. In particular, s. 2(1) of PIPEDA defines "commercial activity" to mean "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists". Although a charity might interpret this to mean that it can provide (*e.g.,* give for free instead of sell, barter or lease) its donor, membership or other fundraising lists to its parallel foundation to do fundraising on its behalf, it is generally not advisable for the following reasons:[6]

- The Privacy Commissioner of Canada makes a distinction between "transfer" and "disclosure". An organization can only "transfer" personal information to a third party without the individual's consent for processing purposes if the organization remains responsible for the actions of the third party and stringent conditions are met. An organization cannot "disclose" personal information to a third party without the individual's consent.[7]
- The Alberta, British Columbia and Québec provincial legislation does not permit a charity to do

so without consent even for non-commercial purposes.

- The Ontario provincial legislation does not permit a charity to do so without consent when using an individual's personal health information.
- Even in limited situations where a charity is not subject to privacy legislation, it is still important for the charity to adhere to the underlying privacy principles. In this day and age, the public expects charities to recognize that an individual's right to privacy is an essential issue.

Alberta, British Columbia and Québec provincial legislation

Provincial legislation in Alberta, British Columbia and Québec requires consent for the collection, use and disclosure of personal information, regardless of whether or not it is for commercial purposes. In addition, charitable and non-profit organizations in these provinces may also still be subject to PIPEDA under certain circumstances, as PIPEDA will continue to apply to all commercial activities relating to the exchange of personal information between provinces and territories and to information transfers outside of Canada.[8]

Ontario provincial legislation

Provincial legislation in Ontario requires consent for the collection, use and disclosure of personal health information. In particular, s. 32(1) of Ontario's *Personal Health Information Protection Act* specifies that charitable and non-profit organizations, whether they are the health information custodian (*e.g.*, hospital) or an agent acting on the health information custodian's behalf (*e.g.,* foundation), may collect personal information for the purpose of fundraising only either (1) with the individual's express consent, or (2) with the individual's implied consent if the collection is restricted to the individual's name and mailing address. Any other information, such as telephone numbers, may only be collected with the individual's express consent. This means that the organization cannot use the name and mailing address provided by the individual to obtain the individual's telephone number through publicly available directories in order to contact the individual for fundraising purposes. This is because the information provided can only be used for the purpose authorized at the time of collection, and it is unlikely that individuals would have authorized the collection of their names and mailing addresses for the purpose of tracking down their telephone numbers.[9]

Therefore, before a charitable or non-profit organization even calls or mails an individual to solicit funds or volunteers, it will usually need to have the individual's consent to collect, use and disclose the personal information required for the call or mail.

U.S. Anti-Terrorism Legislation

Having said the above, charitable and non-profit organizations need to be aware that the time, effort and costs spent on obtaining consent may be thwarted if the personal information is transferred to a U.S. organization, such as where a database of personal information resides on a computer located in the U.S.

While Canadian privacy legislation allows the collection, use and disclosure of personal information if proper arrangements are first made for its protection in Canada, once the personal information enters U.S. jurisdiction, legislation such as *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (the "PATRIOT Act") provides U.S. authorities with the means to access that personal information.[10] In particular, the Federal Bureau of Investigation (FBI) can obtain court orders to access personal information held in the U.S. or within the control of a U.S. entity without the consent of the individual. This means that Canadian charitable and non-profit organizations possessing databases of personal information, in paper or electronic format, that enter U.S. jurisdiction (whether by travelling to a U.S. jurisdiction with that information, storing the information on a computer or server hard-drive or other storage device located in the U.S., sending the information for processing in the U.S., or disclosing it to a third party in the U.S.) will have lost control of the personal information under the compulsion of the U.S. government.

As a result, any protection afforded by Canadian privacy legislation for personal information collected, used and disclosed in Canada will be undermined by the PATRIOT Act once that personal information flows across the border into U.S. jurisdiction. In this regard, charitable and non-profit organizations should take the following steps to protect their donors, supporters, members, employees, volunteers and themselves:

- Ensure that all personal information is kept in Canada. This means ensuring that all paper copies and electronic storage devices having copies of the information (*e.g.*, computers, servers, and portable storage devices, including universal serial bus (USB) drives, compact discs (CDs) and digital video discs (DVDs)) remain in Canada, that all personal information is processed in Canada, and disclosing personal information to third parties in Canada only, etc.
- Where the above is not possible due to an affiliation with a U.S. entity, or because the related services can only be provided in the U.S., etc., it is imperative that charitable and non-profit organizations only permit U.S. entities to access limited personal information on a "need-to-know" basis and require that it be deleted and destroyed once that use is no longer required.
- Furthermore, it is imperative that the charitable and non-profit organization disclose to individuals that their personal information could be subject to the PATRIOT Act, in order to permit the individuals to make an informed decision concerning whether or not they wish to permit the organization to collect, use and disclose their personal information.

Position of the Privacy Commissioner of Canada

Charitable and non-profit organizations should be aware of the importance that the Privacy Commissioner of Canada has placed on this issue in its fact sheet, which was published on August 18, 2007 and is available at <http://www.privcom.gc.ca/fs-fi/02_05_d_23_e.asp>.

In reminding organizations of their obligations under Canadian privacy legislation to ensure the security of personal information, the Privacy Commissioner of Canada also advised Canadians to take the following steps to protect themselves:

- By bringing complaints about the handling of personal information (especially outsourcing arrangements) to the Office of the Privacy Commissioner of Canada or provincial and territorial commissioners, depending on the organization whose conduct has raised the concern;
- By relying on the "whistle blowing" provisions of PIPEDA if a US-based affiliate of a Canadian organization seeks to reach into Canada to obtain personal information held in a Canadian database in order to comply with a US legal order. These provisions would protect the confidentiality of employees who notify the Privacy Commissioner of Canada that a company intends to transfer information abroad in violation of PIPEDA. The provisions also protect employees against retaliation by the employers, such as harassment, dismissal or demotion;
- By letting organizations in Canada that collect personal information about Canadians know that there is a concern about personal information being processed outside Canada;
- By taking advantage of the information rights existing under PIPEDA and provincial private sector statutes which require organizations to follow fair information practices, notably obtaining consent for information use;
- By reminding companies in Canada of their legal obligation to introduce appropriate security measures to prevent their subsidiaries or affiliates in another country from secretly obtaining access to personal information held in Canada to comply with a court order made in the foreign country;
- By raising their concerns about the potential for excessive disclosure of personal information to foreign governments or to foreign companies with their elected representatives; and
- Generally, by being more attentive to what may be happening to their personal information when it crosses borders and to the importance of clear and enforceable international standards on information sharing in democratic countries.

Concluding Comments

While all individuals have a part to play in protecting personal information, charitable and non-profit organizations must take the initiative to educate and protect their donors, supporters, members, employees, volunteers and themselves about the importance of protecting personal information and the consequences of transferring such information beyond Canadian borders.

Editor's note: U. Shen Goh practices in the areas of intellectual property and privacy law from the Mississauga office of Carters Professional Corporation More information can be found at <www.carters.ca.>

* This article was first published in the *Charity Law Bulletin* No. 128, November 29, 2007, Editor, Terrance S. Carter, available at <http://www.carters.ca/pub/bulletin/charity/2007/chylb128.htm>.

[1] M.H. Hall, M.L. de Wit, D. Lasby and D. McIver, *Cornerstones of the Community: Highlights of the National Survey of Nonprofit and Voluntary Organizations* (Ottawa: Statistics Canada, 2004), at 7.

[2] *Ibid*., at 10.

[3] *Ibid*., at 9.

[4] *Ibid*.

[5] S.C. 2000, c. 5.

[6] For more detailed discussions on the definition of "commercial activity" and the applicability of PIPEDA to charitable and non-profit organizations, please see *Charity Law Bulletin* No. 28 "Impact of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) on Charitable and Non-profit Organizations"; *Charity Law Bulletin* No. 42 "Update on the Application of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to Charitable and Non-profit Organizations"; and *Charity Law Bulletin* No. 97 "Update on the Application of PIPEDA to Municipalities, Universities, Schools and Hospitals".

[7] For more detailed discussion on the differences between "transfer" and "disclosure" of personal information and the obligations set out in PIPEDA, please see *Charity Law Bulletin* No. 71 "Privacy Policy Not Enough, 3rd Party Privacy Contract Also Needed To Comply With PIPEDA".

[8] For more detailed discussions on provincial legislation, please see *Charity Law Bulletin* No. 70 "Privacy Legislation Increasingly Applied to Charitable and Non-profit Organizations".

[9] For more detailed discussions on Ontario's *Personal Health Information Protection Act*, please see *Charity Law Bulletin* No. 95 "Privacy Legislation and Its Application to Fundraising and Personal Health Information".

[10] For a discussion of the anti-terrorism information collection and sharing in Canada, please see *Anti-terrorism and Charity Alert* No. 12 "New Anti-Terrorist Financing Law has Direct Impact for Charities".