Title: "Sharing Data and Protecting Privacy: A Case Study from Alberta"
Author: Kiran Pohar Manhas, Jason Lau and Xinjie Cui
Published in: *The Philanthropist*, Journal
ISSN 2562-1491
Date: November 27, 2017
Original Link: https://thephilanthropist.ca/2017/11/sharing-data-and-protecting-privacy-a-case-study-from-alberta/
Date of PDF Download: June 22, 2019

Sharing Data and Protecting Privacy: A Case Study from Alberta

By Kiran Pohar Manhas, Jason Lau and Xinjie Cui

The internet has changed how we consider information: vast amounts of it are available, information accessibility is amazingly rapid, and digitalized information is immediately ready for machine use (Lenczner, 2012). Companies are directed to view in-house data as critical to achieving "a sustainable competitive advantage" (Niemi, 2013, p.1). The internet and emerging technologies facilitate and promote data re-use and re-purposing in multiple ways that often diverge from the original purposes at collection.

Thus, many actors are increasingly considering the availability and opportunity of data, including those working in the public, research, private, and non-profit sectors. Where information about people is concerned, privacy obligations arise legally and ethically. We conducted research into the privacy obligations and practices that accompany data re-use and re-purposing for non-profit organizations in Alberta.

Why data matters to non-profits

A study of 12 non-profit organizations demonstrated that high-impact, successful organizations, amongst other things, used information to change tactics and increase success (McLeod Grant, 2007). Data measures organizational impact, as well as financial and operational health, and it identifies problems (Idealware, 2012). Data analysis can improve understanding of needs, results, and impact, as well as operational effectiveness (de Las Casas, 2013). In 2016, two major trends for Canadian non-profit organizations included (a) using novel technologies and data management tactics to maximize impact and promote efficiency, and (b) greater reliance on shared platforms and administrative outsourcing to weather a challenging economy (Cave, 2016).

The Nonprofit Technology Network surveyed non-profits to find out the types of data they use (Idealware, 2012). They include:

- Financial and internal operations data (e.g. expenses, income, volunteer hours);
- Marketing, communications, and fundraising data (e.g. mailing list numbers; new donor numbers; website traffic; Facebook comments);

- Tracking programs and outcomes (e.g. financials versus budget; attendance data; client demographics and outcomes; client recidivism); and
- External data (e.g. related open government data and aggregate or individual-level data from other non-profits).

Program and service data also inform a non-profit organization's health and success. These myriad data could advance decision-making for non-profit organizations.

In studying domestic non-profits, Canadian researchers are viewed as behind other countries (Lenczner, 2012). Lack of non-profit data may contribute to this (Ibid). There are many calling for non-profit organizations to facilitate data re-use, including publishing data in easier-to-use formats, in non-aggregated or non-summary form, and with explicit permission for re-use (Van Ymeren, 2015, Lenczner, 2012, Cave, 2016, Idealware, 2012, Network, 2015).

Data sharing can be available widely and publicly, or on a restricted basis. Open data is publicly available to anyone with the interest and capacity to utilize it (Van Ymeren, 2015). To meet the principles of openness, data must be "available under an open license; available in a convenient and modifiable form; machine-readable; accessible as a whole, with little or no cost associated with its use" (Ibid). Open data cannot identify individuals (Lenczner, 2012). Meanwhile, shared data is available on a restricted basis beyond original collectors/producers using access processes and agreements (Van Ymeren, 2015). Data repositories are centralized platforms that store and manage shared data. Shared data offers security and privacy protections to facilitate the sharing of information that is too sensitive for open data (e.g. information about individuals).

What challenges do non-profits face in data use and shared re-use?

Accurate data use and re-use requires capacity, skills, and resources. Data about individuals triggers privacy concerns and obligations that must be recognized and protected. This is especially true for sensitive information, such as health, family, or financial information. The non-profit sector is often privy to such personal information. The diverse array of non-profit organizations in Canada includes staff across a spectrum of capacities, skills, resources, and understandings about data use, utility, and privacy laws. This inconsistency – and often dearth of knowledge – present hurdles to getting non-profit organizations "data-ready."

Supply and demand issues impede many non-profit organizations from getting the most out of data (de Las Casas, 2013). Supply issues include legal barriers (e.g. identifying data); technical barriers (e.g. databases' structure and data location); attitudinal barriers (e.g. resistance to data sharing or overriding misuse concerns); and resource-based barriers, such as lack of time, skills, and funds.

Demand-related issues include lack of awareness; lack of capacity or resources to invest; lack of capability for data analysis and interpretation; fear of potentially negative results; and lack of incentives to overcome barriers (Ibid).

For many, surrounding circumstances promote risk aversion and disincentivize data use. Such disincentives include decreased funding, intense competition for resources, greater results-related payments, and a culture ready to criticize non-profits (Ibid).

What we did

In response to the opportunities and challenges of data in the non-profit sector, PolicyWise for Children & Families (PolicyWise) – a provincial non-profit corporation in Alberta, focused on mobilizing evidence to inform social policy by bridging between government, academia, and community – pursued two initiatives (Families, 2017a).

First, it launched a centralized data repository called SAGE – Secondary Analysis to Generate Evidence, in November 2016 (Families, 2017b). SAGE acts as a data and research platform, as well as a resource to researchers and non-profit organizations, to advance and equalize data-use capacity and resources across sectors.

Second, during SAGE development, PolicyWise commissioned an analysis on the legal obligations and ethical responsibilities of non-profit organizations that aim to mobilize collected data from clients. This data is either for further internal analyses or for facilitated connections between non-profit organizations and researchers to leverage analytical capacity to inform evaluation and increase outputs. Privacy obligations were of particular concern to non-profit-sector stakeholders working with SAGE, so the analysis focused on privacy law.

We conducted a thorough review of:

- Key Alberta privacy laws such as the Personal Information Protection Act (PIPA); Health Information Act (HIA); and Freedom of Information and Protection of Privacy Act (FOIP);
- Provincial policy documents that guide implementation of privacy laws (e.g. Service Alberta's "A Guide for Businesses and Organizations on the Personal Information Protection Act");
- Key federal privacy laws (the Personal Information Protection and Electronic Documents Act (PIPEDA), and related regulations);
- Relevant Alberta court decisions; and
- Thirty-six decisions of the Office of the Information and Privacy Commissioner of Alberta (OIPC), issued between 2012 and 2017.

We supplemented this legal information with academic and grey literature around best practices on data sharing and privacy protection, particularly for non-profit organizations.

What we found

We learned three key things: (a) privacy laws do not apply universally or uniformly to non-profit organizations; (b) the three major features of a balanced approach to data use and privacy protection include reasonableness, consent, and minimal extent possible; and (c) privacy laws and international principles offer guidance on best privacy practices.

Legal obligations only apply if an organization falls under the law's jurisdiction. Non-profits must first consider whether they fall under the HIA, FOIP, or PIPA.

A non-profit organization is bound by the HIA if:

- The organization is defined as an HIA custodian (e.g. it's a health system or board, hospital, or a listed health professional);

- The information at issue is personal health information (e.g. defined to include information about a condition and about a person);
- The information was collected, used or disclosed during a health service; and
- The information was recorded (2000b, Alberta, 2011).

When these criteria are met, the non-profit organization must comply with HIA rules and processes.

If the HIA does not apply, a non-profit organization must determine if it is bound by FOIP: privacy legislation governing public sector institutions in Alberta (2000a). If the non-profit organization is a public body, or a contractor of a public body, then it is bound by FOIP in its information-handling processes.

Finally, non-profit organizations that do not fall under HIA or FOIP must consider whether they are governed by the private-sector privacy laws in Canada: the federal PIPEDA and the provincial PIPA. For private-sector organizations that operate wholly within Alberta, only PIPA applies; Alberta organizations that include operation across borders are subject to PIPEDA for trans border activities. There are two ways non-profit organizations trigger PIPA attention. If the organization's incorporation status does not meet the "not-for-profit" exceptions listed in PIPA, then PIPA applies to all the organization's activities and information handling. When a non-profit organization is duly incorporated under the Societies Act, the Agricultural Societies Act, or Part 9 of the Companies Act, it is considered a not-for-profit organization under PIPA and only "commercial activities" involving the collection, use, or disclosure of personal information are subject to PIPA.

Non-profit organizations can face dynamic privacy obligations that apply to all, some, or none of their information-related activities for all, some, or none of the time. This has created confusion across the non-profit sector in Alberta and contributed to a national culture of reticence to consider data re-use (Lenczner, 2012, Idealware, 2012, Van Ymeren, 2015).

What do privacy laws require?

It is beyond this article's scope to detail the legal obligations of HIA, FOIP and PIPA. We can, however, provide general guidance on key privacy obligations in Alberta, which has some of the most stringent privacy laws in Canada. For more detail, our full research report is available online through PolicyWise (Manhas, 2017).

Legal obligations under privacy laws only apply to personal information. Information that has been stripped of any identifying information (i.e. de-identified) or that is at a group-level (i.e. aggregated) is exempt from privacy laws. However, with advances in technology and the availability of diverse datasets, de-identified information retains a risk of re-identification (Ohm, 2010). This dynamism calls for regulatory flexibility by OIPC and cautious, case-by-case risk assessments by public- and private-sector organizations.

Privacy laws are focused on information handling activities, particularly information collection, use and disclosure. Information "use" legally means handling or analysis internal to an organization and includes contractors; information "disclosure" encompasses any handling or sharing external to an organization (2008). For non-profit organizations, all information handling and analysis wholly internal to their organization or to contractors is a "use," while handling, analysis or sharing beyond the organization must follow disclosure rules in applicable privacy laws. Sharing of non-profit data with an

external data repository, without a contractual agreement, would be disclosure.

Privacy laws aim for a reasonable balance between an organization's need to collect, use, or disclose information for reasonable purposes against the individual's right to have their personal information protected (2003, 2000a, 2000b). For PIPA, reasonableness means "what a reasonable person would consider appropriate in the circumstances" (2003, 2008). Being nonchalant about individuals' identities and intimate details is unreasonable, but so is being completely closed to potential learnings from analyzing organizational- and individual-level data (McKinley, 2013). Promoting service and sector efficiency through data use and disclosure for a private sector organization, including non-profit organizations, when privacy protections are in place, would be reasonable (McKinley, 2013).

When the OIPC or courts consider privacy complaints around personal information handling, the legal question is whether the information handling was authorized. Data is used if it is available for consideration internally, not whether the data was given any, little, lots, or no weight during the handling activity. Information does not have to be relied upon to be used. Data is disclosed when someone external to the necessary parties could view it; whether they actually viewed it does not impact the legal analysis.

Three key, interrelated factors should guide organizational collection, use and disclosure of information: consent, purpose, and reasonableness.

- A reasonable purpose must exist for information collection.
- Consent, or statutory exemption to consent, must be gained and must connect to the reasonable purpose.
- Information should only be used and disclosed to the minimal extent needed to meet the reasonable purpose.
- The connections between purposes and activities should be direct and reasonable.

The minimal amount of personal information should be used or disclosed (even if authorized to collect more). Uses or disclosures of individually-identifying information should only occur when aggregate or de-identified data do not suffice. Everyone should operate on a "need to know" basis.

Unless there are legal exemptions, organizations must get informed consent to collect, use, or disclose personal information. Organizations must inform individuals of the purpose for information collection, as well as the proposed and potential uses, disclosures, storage, and disposal of the information (2008). Consent can be express (written or verbal), implied (information is volunteered in reasonable and clear circumstances), or opt-out (Ibid). Unless a legal duty or obligation would be hindered, individuals must be able to change/withdraw consent with reasonable notice and/or place reasonable provisos to their permission (e.g. limit types of re-use) (2008, 2003).

Databases can contain a wealth of personal information and should be safeguarded appropriately. Access to information in databases, and the reasons for such accesses, should be appropriately logged; and all parties who do, or could, access data should have proper privacy training; and, privacy compliance should be monitored.

Failure to comply with provincial privacy laws can lead to complaints, monetary sanctions, and/or OIPC orders.

Privacy protection laws do not aim to limit information exchange with anonymity provisos around service delivery itself; but aim to limit and safeguard information exchange beyond point of care. Any initial point of care and service delivery likely involves information collection as necessary; but any information re-use must involve the highest levels of anonymity possible.

Beyond the law, what are best practices in data governance?

Non-profit organizations engaged in non-commercial activities and not connected to the HIA or FOIP are not legally bound by any privacy law, including PIPA. However, we highly recommend non-profit organizations to adhere to PIPA guidelines and privacy best practices. This would promote a privacy-protecting culture, avoid costs and confusion associated with dynamic privacy law applicability, and avoid reputational and non-legal costs when information is handled inappropriately.

Globally, the Fair Information Principles, originally espoused by the Organization for Economic Co-operation and Development in 1980 (Development, 2011), guide all privacy laws. These eight principles call for:

- The necessity of consent to lawfully collect, use, and disclose personal information;
- Accuracy, completeness, and currency of personal data;
- Purposes to direct personal data consent and handling;
- Appropriate security measures safeguarding personal data;
- Transparency so individuals can see and correct information collected about them; and
- Openness and accountability around fair data use by data controllers (Development, 2011, 2008).

These principles enable treating all potentially-identifying information with a universal privacy-protecting approach.

Information handling best practices, as demonstrated by the Fair Information Principles, privacy laws, and industry best practices include the following (Berens, 2016; Karunakara, 2013; Folkes, 2013; Network, 2015, Network, 2016; Foundation, 2015; McCort, 2015):

- Instituting an organizational privacy policy including visions and values on privacy protection and data mobilization;
- Appointing a privacy officer to ensure policy compliance;
- Ensuring consent is obtained from individuals for personal-information handling;
- Ensuring the purposes of information collection, use, and disclosure are clear and reasonable;
- Ensuring the adequate security of information; and
- Elaborating the access and correction processes, including individual and organization responsibilities.

What does this mean for non-profit organizations?

In a world where data is considered an innovation and asset, and where many commercial entities, especially in social media, harvest the data provided to them and leverage it for profit, the public is increasingly concerned about their information, who has access to it, and what people are doing with it. Nonchalance about privacy is an inappropriate approach.

As confusing as the legal landscape can appear, it offers guidance in-line with best practices on data governance. Best practices come from clear legal obligations of other more-regulated sectors (e.g. private-sector businesses, public bodies, and health-information custodians), and from industry standards from the non-profit sector itself. The trifecta of purpose, reasonableness, and minimal extent appear throughout privacy laws in Alberta and non-profit privacy best practices. Adhering to privacy best practices would not present significant costs to organizations; would avoid inefficiencies of having different information-handling procedures for different activities (e.g. commercial vs. non-commercial activities); and would limit the risk of negative publicity and lost public trust from privacy complaints (McKinley, 2013).

References

2000a. Freedom of Information and Protection of Privacy Act. Canada: Statutes of Alberta.

2000b. Health Information Act. Canada: Statutes of Alberta.

2003. Personal Information Protection Act. Canada: Statutes of Alberta.

2004. A Guide for Businesses and Organizations on the Personal Information and Privacy Acti. Edmonton, AB: Service Alberta.

Government of Alberta. 2011. Health Information Act: Guidelines and Practices Manual. Edmonton, AB.

Berens, J., Mans, U., Verhulst, S., 2016 *Mapping and Comparing Responsible Data Approaches*. GovLab and Centre for Innovation, Leiden University.

Berger, M.L., Lipset, C., Gutteridge, A., Axelsen, K., Subedi, P., and Madigan, D., 2015 *Optimizing the leveraging of real-world data to improve the development and use of medicines*. Value Health, 18, 127-30.

Cave, J., 2016 ‘A shifting sector: emerging trends for Canada’s non-profits in 2016.’ *The Philanthropist*.

IBM Knowledge Center. 1990, 2014. Data Sharing Concepts and Terminology. z/OS MVS Programming: Sysplex Services Guide. IBM Corporation.

Committee on Transborder Flow of Scientific Data, N. R. C. 1997. Bits of power: Issues in global access to scientific data.

De Las Casas, L. G., T.; Pritchard, D., 2013. *The Power of Data: Is the Charity Sector Ready to Plug In?* London, UK.

Organization for Economic Cooperation and Development , 2011. Thirty Years After: The OECD Privacy Guidelines. Paris.

PolicyWise for Children & Families, 2017a. PolicyWise for Children & Families [Online]. Edmonton. Available: https://policywise.com/ [Accessed 01 August 2017 2017].

PolicyWise for Children & Families, 2017b. SAGE – Secondary Analysis to Generate Evidence

[Online]. Edmonton, AB: PolicyWise for Children & Families. Available: https://policywise.com/initiatives/sage/ [Accessed 01 August 2017 2017].

Folkes, C. 2013. Understanding Non-profit Data Governance [Online]. LinkedIn. Available: https://www.slideshare.net/CathyFolkesCFRE/understanding-non-profit-data-governance [Accessed May 15, 2017 2017].

Vancouver Foundation, 2015. Open Licensing Initiative [Online]. Vancouver: Vancouver Foundation. Available: https://www.vancouverfoundation.ca/our-work/initiatives/open-licensing-initiative [Accessed Mar 22, 2017 2017].

Idealware 2012. The State of Non-profit Data. Portland, OR.

Social Sciences and Humanities Research Council, Canadian Institutes for Health Research, Natural Sciences and Engineering Research Council, and Canadian Foundation for Innovation, 2014. Capitalizing on Big Data: Toward a Policy Framework for Advancing Digital Scholarship in Canada. Ottawa.

Karunakara, U., 2013. Data Sharing in a Humanitarian Organization: The Experience of Médecins Sans Frontières. PLOS Medicine, 10, e1001562.

Lenczner, M. P., S., 2012. From Stories to Evidence: How Mining Data Can Promote Innovation in the Non-profit Sector. Technology Innovation Management Review, 10-15.

Manhas, K. P., 2017. Law & Governance of Secondary Data Use: Obligations of Not-for-Profit Organizations in Alberta. Edmonton, AB: PolicyWise for Children & Families.

McCort, K., 2015. Open Policies Unlock Our Full Potential [Online]. Vancouver: Vancouver Foundation. Available: https://www.vancouverfoundation.ca/whats-new/open-policies-unlock-our-full-potential [Accessed March 22, 2017 2017].

McKinley, A. 2013. The Effect of Privacy and Anti-Spam Legislation on Charities and Non-Profits. Advising Charities, Not-for-Profits and Social Enterprises 2013/2014 (Seminar). Calgary, AB: Legal Education Society of Alberta.

McLeod Grant H., Crutchfield, L.R., 2007. Creating High-Impact Non-profits. Stanford Social Innovation Review, Fall 2007, 32-41.

Ontario Nonprofit Network. 2015. Towards a Data Strategy for the Ontario Non-profit Sector. Toronto, ON.

Ontario Nonprofit Network. 2016. Data Strategy [Online]. Toronto: Ontario Non-profit Network. Available: http://theonn.ca/our-work/our-partnerships/data-strategy/#1467045087069-8c6d1de7-a236 [Accessed March 24, 2017 2017].

Niemi, E., 2013. Designing a Data Governance Framework. IRIS, the Scandinavian Chapter of the Association for Information Systems.

Ohm, P., 2010. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.

UCLA Law Review, 57, 1701-1777.

Van Ymeren, J., 2015. An Open Future: Data priorities for the not-for-profit sector. Toronto, ON: The Mowat Centre's Not-For-Profit Research Hub.

Illustration by Paul Dotey