P.O. Box 2596, Station D, Ottawa, ON K1P 5W6 phone 613 234-6977 fax 613 234-8500
email aca@archivists.ca www.archivists.ca

Association of Canadian Archivists
Association canadienne des archivistes

Association of Canadian Archivists Appearance before the ETHI Committee hearing on the Personal Information Protection and Electronic Documents Act (PIPEDA)

June 1, 2017

Good afternoon and thank you for the opportunity to speak to the Standing Committee on Access to Information, Privacy and Ethics during your hearings on the Personal Information Protection and Electronic Documents Act (PIPEDA).

My name is Greg Kozak and I am here today speaking on behalf of the Association of Canadian Archivists (ACA). I am a professional records manager and also teach as an adjunct professor at the University of British Columbia's School of Library, Archival and Information Studies, focusing on freedom of information and protection of privacy legislation.

The ACA is a national association of professionals that work in both the public and private sector. We have close to 500 members and 200 institutional members across the country. Our scope of interest spans the entire lifecycle of records, both digital and physical, from their creation to their final disposition, whether that is destruction or permanent retention for historical purposes. We are also advocates for consistent, accurate, and transparent information management practices that respect national and international standards. Thus, our membership includes records managers, who look after current records within their organizations, and archivists, who deal primarily with historical records in archival institutions or programs. Often the two responsibilities overlap.

We are interested in providing comments on existing or proposed legislative or regulatory texts that may affect our ability to manage trustworthy records and preserve, control, and provide access to authentic records over the long term.

It is on these points that we would like to focus our remarks.

Trustworthiness of Records

Trustworthy records are records that are created in a way that ensures their accuracy, completeness, and reliability, and then maintained and preserved so that their identity and integrity—their authenticity that is, is unquestionable. Trustworthy records are records that can be used as evidence of the facts and acts they attest or refer to for both legal and research purposes.

In our increasingly digital and connected world, keeping trustworthy records has become more complex. Much of this complexity relates to privacy issues and to the management of personal information. Specifically, we see two areas related to privacy where the trustworthiness of records is challenged. The first is the processing of the data in the creation and maintenance of the records.

P.O. Box 2596, Station D, Ottawa, ON K1P 5W6 phone 613 234-6977 fax 613 234-8500
email aca@archivists.ca www.archivists.ca
Association of Canadian Archivists
Association canadienne des archivistes

In his letter to this Committee, the Privacy Commissioner of Canada, Mr. Therien states: "it is no longer entirely clear who is processing our data and for what purposes."[1] To add to his point, we would like to note that we also do not know *how* our data is being processed, and *by what means*. The growth of visual analytics as a method of analysis and the reliance on complex algorithms mining various data sets for decision making result in a complex web of interactions whose outcome is likely to infringe the privacy of the people whose information was collected. In such situations, good records management is a prerequisite to the protection of privacy as it would control the processing of the data of individuals while ensuring the creation of a reliable record of the actions of those who are entrusted with them.

The second area where the trustworthiness of records is challenged is the use of certain security measures to de-identify personal information contained in records. An example of this is tokenization, whereby a known individual's identity is replaced with another unique non-obvious identifier. The controlling agency retains a table of concordance that permits it to match the unique identifier with the known individual. The issue here is that such security measures are creating records that are difficult to manage over the long term. Again, we can see a convergence between records management and privacy requirements. In order to establish a level of trust over de-identified records, we still need to know what actions were performed on them.

Considering the challenges described above, it is clear that solid information management practices are a foundational element to effective privacy management. Thus, the ACA recommends that organizations be required to include records management capabilities into their processes and systems that encompass privacy needs. This aligns with the direction of the European Union's General Data Protection Regulations, which require Privacy by Design and Default, in other words, records systems designed with keeping privacy in mind.

Preservation of Records

Archivists acquire records that stand as testimony of human action. These records, created by public and private organizations and individuals, span all fields of endeavour—administrative, scientific, legal, financial, and cultural. Archives acquire records that show humanity at its best, its most ordinary, and its worst. Preserving records is a societal good that ensures the historical accountability of one generation to another, and permits the public to access unique sources of information for a broad range of purposes. Such purposes range from historical research to scientific enquiry to addressing past injustices through reconciliation efforts.

[1] Daniel Thierien, Letter to Standing Committee on Access to Inforamtion, Privacy and Ethics, December 2, 2016.

Association of Canadian Archivists
Association canadienne des archivistes

In this regard, the ACA recommends:

- Preserving PIPEDA's existing mechanisms that permit private organizations to donate records containing personal information to archives for long-term preservation,
- Allowing archival institutions or programs falling under PIPEDA to acquire ("collect") records containing personal information, and
- Carefully considering the implications of introducing a right to be forgotten or a right to erasure.

At the moment, PIPEDA permits organizations to donate ("disclose") records containing personal information of long-term value to an archival institution for preservation (s. 7(3)(g)). This mechanism should be maintained to ensure archives are able to acquire and maintain records of private organizations. It is vital that private organization be able to donate their records to ensure the all-of-society representational nature of archival holdings.

One area where PIPEDA could be improved is allowing archival institutions covered by it to acquire records that fall under the archives' mandate. Currently, such archives need consent from the data subjects to acquire ("collect") records containing personal information. In practice, it is very unlikely that organizations would seek consent to allow records containing personal information to be donated to a third-party.

Therefore, the ACA recommends that archival preservation of records be recognized as consistent with the initial purpose for which the personal information was collected. This reflects the approach adopted by the EU's GDPR, where "further processing for archiving purposes… [is] not considered to be incompatible with the initial purposes" of collection (Art. 5(1)(b)). However, the organization must have a bona fide archival mission, consistent with the ACA's Code of Ethics and Professional Conduct, and not have been set up as an archives for the purpose of avoiding the Act.

Third, the ACA believes that, if a right to be forgotten or to erasure were introduced, it would impact the ability of archives to preserve records. It is essential to ensure a careful balance between the protection of an individual's reputation and the integrity and authenticity of the public record. PIPEDA is already based on the principle that personal information be kept accurate, complete, and up-to-date. A wider application of this principle could rectify instances where incorrect or inaccurate personal information may result in reputational harm, reducing the need for a right to be forgotten. Regardless, the test to determine reputational harm must be clear and the bar should be set high enough to remove frivolous or inconsequential requests.

P.O. Box 2596, Station D, Ottawa, ON K1P 5W6 phone 613 234-6977 fax 613 234-8500
email aca@archivists.ca www.archivists.ca
Association of Canadian Archivists
Association canadienne des archivistes

We should also view a right to be forgotten from an historical perspective. Specifically, it is to be considered that personal information becomes less sensitive over time. This is already acknowledged in PIPEDA, where it is established that information about someone who has been dead for more than 20 years or contained in records that have been in existence for longer than 100 years can be disclosed freely. Similarly, the EU's GDPR do not apply to deceased persons. Therefore, reputational harm will diminish over time, and there will be a point when it is causes no harm; thus, the legislator should be mindful of introducing any measure that may irreversibly remove or conceal records.

Cloud Environment

Increasingly, records are created, maintained and/or preserved in cloud environments, which are characterized by location independence. This type of environment was in fact the catalyst for European data protection regulations and is a strong aspect of the drive in several countries towards jurisdictional location requirements for the data related to their citizens.

In Canada, some provinces require that public bodies ensure that personal information under their care or control is stored and accessed only in Canada, subject to legislative exceptions. The Canadian government does not prohibit government institutions under the Privacy Act or organizations under PIPEDA from using a Cloud Services Provider that stores personal information outside Canada, but recommends that privacy risks be identified, including the need for transparency, consent and notification of the individual that the personal information is about.

The ACA believes that PIPEDA should make a definite statement on the issue of jurisdictional location of data of private individuals, otherwise what happens to them will be mostly decided by legal opinion rather than by clear consistent rules.

This concludes our submission.

Thank you again for allowing the ACA to present on this subject.