February 8, 2017

Mr. Blaine Calkins, M.P.
Chair
House of Commons Access to Information, Privacy and Ethics Committee
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Calkins:

The National Association for Information Destruction – Canada (NAID-Canada) looks forward to your Committee's upcoming review of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. Canada has traditionally been a global leader in privacy protection, though in recent years that standing has started to erode as other countries introduce more stringent measures.

In fact, with the new General Data Protection Regulation (GDPR) now law in the European Union, the absence of strong enforcement and reference to meaningful service provider controls in Canada is even more glaring – as is the fact Canada's breach notification law is still not in effect despite being passed over a year and a half ago.

By way of background, NAID-Canada is the national non-profit association representing companies that specialize in secure information and document destruction. NAID-Canada's mission is to raise awareness and understanding of the importance of secure information and document destruction. In doing so, we want to ensure that private, personal and business information is not used for purposes other than originally intended. NAID-Canada also plays an active role in the development and implementation of industry standards and certification and provides a range of member services which include advocacy, communication, education and professional development.

Please find enclosed a package of proposed PIPEDA amendments from NAID-Canada that would address a persistent problem: the failure to safely destroy information that is no longer needed. Our primary recommendation is to include a definition of information destruction in PIPEDA, as well as an explicit requirement for organizations to safely destroy information that is no longer needed.

The recommendation to define destruction was endorsed by the Committee during the last PIPEDA review in 2007, but it did not result in legislative changes. Since then, other countries have continued to take this step, thereby providing their citizens with enhanced

privacy protection. In addition, many jurisdictions, particularly at the State level in the U.S, now impose significant fines on organizations that fail to safely destroy information, which is also something we believe Canada should consider. Here in Canada, jurisdictions like Alberta have given their privacy authorities fining power already.

More information on these issues is provided in the enclosed document and we would welcome the opportunity to appear before your Committee as part of this review.

Finally, please also note that NAID is currently conducting the largest known forensic examination of second hand memory devices, the results of which will be released at our annual conference in March. Several past studies, including one by the Privacy Commissioner of Canada, have found that discarded or recycled electronic devices are often not properly wiped of personal information. The press release announcing this study is attached and we will share the results with the Committee when they are released.

Thank you for your time and consideration, and please do not hesitate to contact me if you have questions about any of these issues.

Sincerely,

K. Backman

Kristjan Backman
Chair, NAID-Canada

cc: Members of the House of Commons Access to Information, Privacy and Ethics Committee
Mr. Hugues La Rue, Committee Clerk

Unveiling Soon: The Largest Second Hand Electronic Device Study

January 25, 2017

NAID has long included research among the tools it uses to educate consumer and policy makers. In fact, over the years, research has contributed to the association's regulatory advocacy and standards development, and added significantly to the association's credibility. In continuation of that tradition, NAID is currently conducting the largest known forensic examination of second hand memory devices, the results of which to be unveiled at the upcoming annual conference.

According to NAID CEO Bob Johnson, this is the type of research that sets NAID apart. "There's no shortage of conferences, magazines, and certifications looking for support," says Johnson. "To my knowledge, however, NAID is the only one with a rich history of reinvesting that economic support back into research to advance and promote secure data destruction."

This study is commissioned by NAID but being conducted by a third party to ensure the reliability and integrity of the results. While there will be no public shaming of organizations (the results will be aggregated), the specific findings will be offered to regulators should they wish to investigate further.

Over the past 20 years there have been periodic studies of used hard drives purchased on the secondhand market. The first known study was conducted between 2000 and 2003, when a team lead by Dr. Simson Garfinkel purchased 158 used hard drives from a number of random sources, which were then subjected to forensic analysis. The results of the study, published in the IEEE Security & Privacy that same year under the title Remembrance of Data Passed, demonstrated that a significant percent of these randomly selected secondhand hard drives contained personal information. As startling as that result was, so was the discovery that the some of the hard drives on which personal information was found had previously been deployed in government, banking, and healthcare, all of which have regulations protecting their associated data. Furthermore, and similarly problematic, many of the hard drives containing personal information showed evidence that someone had attempted to overwrite them. This suggested that the previous owner believed they wiped the drives but had not in actuality.

Canadian-based CHEO Research Institute conducted a similar study in 2007, NAID replicated the study in Australia in 2013, and Blancco Technology Group released a similar study in 2016, all with similar results. In each, regulated or competitive information was discovered on a significant percentage of the hard drives.

The current 2017 NAID second hand device study examines 250 units, including conventional hard drives as well as solid state drives. Among other past NAID research are disposal practice studies conducted in Canada, Spain and the UK, as well as consumer attitudes research in the US and Europe. We feel it is important for NAID members to know the types of initiatives the association dedicates its focus toward. The full results of the current study will be released during the conference at NAID 2017, along with a number of other unveilings, including the first edition of the Information Disposition textbook.

All information destruction professionals are encouraged to attend and be a part of this ground breaking event.

Putting an end to careless data breaches

NAID-Canada believes that information is only as secure as the weakest link in its lifecycle. In too many cases, little attention is paid to the end of a document's lifecycle and its safe destruction and disposal. As evidence of that, there are almost daily reports of personal information being found in dumpsters, recycling bins, abandoned buildings, or stored on discarded computers and other electronic devices. All measures taken to protect that personal information during its useful life are negated if it is not destroyed safely.

As evidence of this problem, in October 2010 NAID-Canada released the results of an audit into information destruction practices in the Greater Toronto Area (GTA). That audit found that 14% of commercial dumpsters in the GTA contained confidential personal information – a shockingly high number. The results for some specific sectors were damning. Of the doctors' offices examined, 75% had left personal information in their publicly accessible dumpsters. For car dealerships, it was 100%.

A new NAID study on recycled electronics will be released shortly.

NAID-Canada has long been advocating for privacy legislation to include a specific destruction requirement, along with a definition of destruction. This is lacking in Canada, but can easily be added through amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). That may be the only way to get organizations to give this often overlooked aspect of privacy protection the attention it is due.

Required Amendments to the *Personal Information Protection and Electronic Documents Act (PIPEDA)*

NAID-Canada recommends PIPEDA be amended to:

- Define destruction as "the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information (or parts thereof) is not practical."
- Add a new clause stating "an organization must destroy personal information when it is no longer needed."

The House of Commons Access to Information, Privacy and Ethics Committee endorsed adding a definition of destruction in PIPEDA when it last reviewed the legislation in 2007. Additional information on how this could be accomplished is detailed below.

Add a definition of destruction

Presently, no definition of destruction is found anywhere in PIPEDA. Therefore, NAID-Canada recommends adding the following to the definitions section of the legislation:

> "Destruction" means the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information (or parts thereof) is not practical. "Destroy" means the act of destruction.

This definition applies to both paper and electronic records. Variations of it have been incorporated into privacy legislation in a number of jurisdictions in Canada, the United States and around the world.

Amending Clause 3 of PIPEDA

Clause 3 of PIPEDA spells out the purpose of the legislation. NAID-Canada recommends amending this Clause as per the underlined section below:

> *The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use, disclosure and destruction of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.*

This amendment would reinforce the fact that organizations need to include a plan for safely destroying personal information in their privacy policy.

Amending Clause 5 of PIPEDA

Clause 5 of PIPEDA should be amended to add a specific destruction requirement. Clause 5 of PIPEDA would then read as follows, with the new section underlined:

> *5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.*
> *(2) The word "should", when used in Schedule 1, indicates a recommendation and does not impose an obligation.*
> *(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.*
> *(4) An organization must destroy personal information when it is no longer needed.*

Our concern here is with Section 4.5.3 of Schedule 1 of PIPEPA that states:

> *Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.*

There are two problems with the above. First is the use of the word "should" in Section 4.5.3. As stated in Clause 5.(2) above, the use of "should" indicates a recommendation and does not impose an obligation. NAID-Canada believes that safe destruction of personal information must be an obligation. It is not something to be left to organizations to decide on their own.

Second, the use of the terms "destroyed, erased or made anonymous" is too vague. We have discussed this matter in the past with Innovation, Science and Economic Development and they have agreed that Section 4.5.3 is open to interpretation.

Therefore, amending Clause 5 as per the recommendation above would make it clear that organizations must destroy personal information when it is no longer needed. They would then have to do so in a manner that meets the criteria spelled out in the proposed definition of destruction.

Restoring Public Confidence

NAID-Canada believes clearly defining destruction is imperative for more than just human rights reasons. It is also a practical necessity. Violating the rights of others by casually discarding their personal information provides much of the feedstock for what has become a global epidemic of identity theft and fraud.

For example, a U.S. study found that the vast majority of identity theft results from low tech access to personal information, such as dumpster diving or binning. Indeed, law enforcement officials in the U.S. have exposed elaborate rings of organized criminals, capitalizing on this ready source of personal information. These rings were found to have divisions of labour, where lower ranks start by harvesting the information from dumpsters, which is then handed over to others of higher rank who have been trained to best exploit it.

That has led to a new generation of legislation in the U.S., exemplified by the *Fair and Accurate Credit Transactions Act (FACTA)* and a host of state laws, which are designed not only to protect privacy rights, but also to stem the tide of identity theft and fraud. As a result, there is a marked difference in the regulatory language regarding information disposal and the penalties for non-compliance.

Where in the past a regulatory reference to information disposal would require limiting unauthorized access, improved regulations now require that steps be taken to destroy personal information prior to its disposal. Further to the point, the newer generation of legislation requires that such security measures be documented in the organization's policies.

Recommendation: Require organizations to have a destruction policy as part of their broader privacy policy.

Building on this point, a January 2016 report of the Information and Privacy Commissioner of Alberta into allegations of improper shredding of documents within the Ministry of Environment and Sustainable Resource Development led to a number of recommendations around information retention and destruction. NAID-Canada wishes to highlight one in particular, namely that the Government "make all operational records schedules available for public review online, which would promote clarity, consistency and full accountability about decision-making for assigning retention policy to government records."

There are potential parallels here for the private sector. For example, if the recommendation above were adopted, it would then be logical to require organizations to publicly post their destruction policy. That would provide an added impetus for organizations to comply while also empowering consumers to identify those businesses that offer the best privacy protection.

Recommendation: Require organizations to publicly post their information destruction policy.

Enforcement and Compliance

Privacy legislation is only as effective as the degree to which organizations comply with it. Closely linked to that is the need to ensure that employees understand and abide by the law. NAID-Canada has found that just having a policy does not necessarily translate into compliance if an organization's employees are not aware of it and/or do not adhere to it.

The keys to the latter are awareness, proper and ongoing training and, where necessary, penalties for violations of the law. Many jurisdictions around the world are moving in this direction, recognizing that certain privacy violations warrant a punitive response.

For example, a medical group in Massachusetts was fined US$140,000 for disposing of 67,000 patient records in a dump without any redacting or shredding.[1] In another case the U.S. Department of Health and Human Services reached an $800,000 settlement with an Ohio company that left 5,000-8,000 patient records in the driveway of a physician.[2] Also in the U.S., the Federal Trade Commission (FTC) fined a Las Vegas real estate broker $35,000 for leaving 40 boxes of customer tax returns, bank statements, consumer reports and other financial records in a public dumpster.[3] Meanwhile, a Missouri medical company faced fines of up to $1.5 million for leaving medical records in a public dumpster.[4]

When it comes to information destruction, there is no excuse for failing to ensure documents are destroyed in a safe and secure manner. As the cases above demonstrate, the U.S. and State Governments take this matter very seriously and have been imposing significant fines.

Recommendation: Empower the Privacy Commissioner to impose fines for egregious or systemic privacy breaches.

Canada's Lost Leadership

Canada used to be regarded as a global leader when it comes to privacy protection. However, that distinction has waned as other countries adopt more stringent privacy protections. Within our own sphere of information destruction, we have documented above the greater clarity required in other jurisdictions around what constitutes destruction as well as the significant fines for failing to safely destroy information that is no longer needed.

NAID-Canada believes that the amendments proposed here would restore Canada's leadership and, more importantly, give Canadians the enhanced privacy protections enjoyed in other countries.

---

[1] See https://nakedsecurity.sophos.com/2013/01/15/medical-patients-health-records-dump/
[2] See http://www.hhs.gov/about/news/2014/06/23/800000-hipaa-settlement-in-medical-records-dumping-case.html#
[3] See http://www.lexology.com/library/detail.aspx?g=5af8a709-0850-487d-bc74-4db192e80ff1
[4] See http://www.hipaajournal.com/hipaa-settlement-reached-dumpster-phi-exposure/