i-SIGMA™

Home of NAID & PRISM International

May 30, 2024

Mr. Garth Rowswell, M.L.A.
Chair
Standing Committee on Resource Stewardship
Legislative Assembly of Alberta
9820 – 107 Street NW
Edmonton, Alberta
T5K 1E7

Dear Mr. Rowswell:

On behalf of the International Secure Information Governance and Management Association (i-SIGMA), please find below our comments on possible reform of the *Personal Information Protection Act* (PIPA). We thank your Committee for the opportunity to provide feedback on the important issue of privacy protection for Albertans.

By way of background, i-SIGMA was created in May 2018 following the merger of the National Association for Information Destruction (NAID) and PRISM International (Professional Records and Information Services Management). NAID has always been the watchdog association for secure shredding operators worldwide and together with PRISM International the joint association now represents all four pillars of records and information management: physical records and information storage; data protection and media vaulting; digitizing and scanning; and confidential records and information destruction services. As such, i-SIGMA is the umbrella association for these professional privacy practices that stand united, heralding the proper information lifecycle management needed in a world of increasing threats to privacy.

Please find below our comments on the issues raised in the discussion paper provided by the Committee.

Changing Legislative Landscape in Canada and Internationally

Privacy protections continue to evolve along with technology and society, though the evolutions of the latter tend to move at a much faster pace than the legislative frameworks. Regardless, the PIPA review is well-timed, allowing you to survey recent developments across jurisdictions and adopt the best measures to bring to Alberta.

We cover some of these later in the submission, including Quebec's requirement to have a privacy management program and improvements to breach notification requirements detailed in a 2021 white paper on privacy reform in Ontario.

i-SIGMA – Canada Office
190 O'Connor Street, 5th Floor, Ottawa, Ontario, K2P 2R3
Phone: 613-241-6000, ext 223
www.isigmaonline.org

In the meantime, one area not covered in the discussion document but which we think worthy of consideration is codes of practice. The 2021 white paper in Ontario proposed having the Information and Privacy Commissioner certify codes of practice. At the federal level, Part 2 of Bill C-27, which is currently before Parliament, would allow entities to apply to the Privacy Commissioner for approval of codes of practice or certification programs.

i-SIGMA has both codes of practice and certification programs and it would be wonderfully simple, particularly for small and medium-sized businesses who outsource data management functions, to be able to ensure their compliance by using a service provider that has a code or certification program approved by the Commissioner, and we therefore encourage Alberta to consider this concept. This becomes even more relevant if Bill C-27 is eventually passed by Parliament as it would deliver the same benefit to Alberta businesses that those covered by federal law will enjoy.

Application

We support extending PIPA to all non-profit organizations and political parties. It is naïve to think those seeking to exploit privacy vulnerabilities will confine their efforts to the sectors already covered by PIPA. Any organization that handles personal information is a potential target. Criminals do not care if you are a business creating a perceived social harm, a non-profit trying to combat that social harm, or a political party seeking to legislate against it; all they care about is accessing personal data for their own profit.

Therefore, all non-profit organizations that handle personal information must be covered by privacy law. While this does come with a modest compliance cost, it is far less than these organizations could face from reputation damage or litigation if they are subject to a major privacy breach.

Finally, political parties should also be covered as they handle vast amounts of personal data. There is something very discordant about political parties not being covered by PIPA when they set the rules for the rest of society and the economy.

Privacy Management Programs

i-SIGMA is very supportive of requiring organizations to have privacy management programs and to require that these be posted publicly. Quebec's new legislation has such a requirement:

3.2. Any person carrying on an enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information. Such policies and practices must, in particular, provide a framework for the keeping and destruction of the information, define the roles and responsibilities of the members of its personnel throughout the life cycle of the information and provide a process for dealing with complaints regarding the protection of the information. The policies and practices must also be proportionate to the nature and scope of the enterprise's activities and be approved by the person in charge of the protection of personal information. These policies must be published on the enterprise's website or, if the enterprise does not have a website, made available by any other appropriate means.

Federal Bill C-27 also includes a requirement for organizations to have a privacy management program. Equally important, that Bill details the information organizations must make "readily available" about how they are complying with the Act. However, it is not clear if this information would have to be publicly posted, as under Quebec law.

We believe public posting is a critical consumer confidence measure as it allows consumers to assess an organization's privacy policies and take their business to those they feel have the best practices.

Privacy Impact Assessment

Generally speaking, i-SIGMA does not object to the notion of requiring organizations to complete and submit a privacy impact assessment to the Information and Privacy Commissioner for specific initiatives involving personal information. However, we note one of the examples offered is when "an organization uses a service provider and there is information sharing outside the organization."

This may present practical and operational challenges. Consider that the Government's economic dashboard reports there are over 120,000 businesses in Alberta. Now imagine if each one had to submit for approval a privacy impact assessment for routine outsourcing practices like data storage or destruction. The Information and Privacy Commissioner's office would be inundated with paperwork and consumed with clerical tasks of questionable benefit to actual privacy protection.

Therefore, if the Committee feels privacy impact assessments should be added to the legislation, there should be some parameters around it to ensure routine business transactions are not ground to a halt. Alternatively, if codes of practice or certification programs are recognized by the Commissioner, per our recommendation above, that could be an alternative. In other words, if you outsource to an entity that abides by a code of practice or is certified by a recognized industry association, you do not have to file a privacy impact assessment.

Breach Notification

Breach notification laws are now a reality across most of Canada and around the world and are something i-SIGMA has supported in all jurisdictions. Alberta should be commended for being ahead of the game with breach notification.

That said, the 2021 Ontario white paper on privacy reform goes a step further. While not all breaches may require notification to affected individuals, it proposed that the Information and Privacy Commissioner should always be apprised so data can be obtained on how breaches are happening. That allows the data on breaches to be reviewed regularly to identify the most common causes, empowering the Commissioner to issue guidance to address those causes if they appear systemic. The Ontario white paper also proposed to make it an offence to not track this information or report it to the Commissioner, something Alberta should consider.

Administrative Monetary Penalties

We support providing the Information and Privacy Commissioner with the authority to impose administrative monetary penalties. 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. i-SIGMA 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. 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.

Such penalties can be severe. For example, looking just at destruction, 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 US$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 fined a Las Vegas real estate broker US$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 US$1.5 million for leaving medical records in a public dumpster.[4]

On the electronic side, Morgan Stanley paid a $6.5 million fine to six U.S. states after it failed to ensure personal information was property removed from computers sent for decommissioning.[5]

This is not to suggest all privacy violations are the same and should be subject to large fines. It is important to distinguish between those that are systemic and/or truly careless versus those that may be due to honest human error. While the latter still need some type of sanction, the focus should really be on systemic problems and gross negligence.

Privacy and Cybersecurity

Cybersecurity is top of mind these days and there is a direct link to privacy protection. In fact, strengthening privacy protections around electronic devices could have the added benefit of improving cybersecurity.

For example, in 2017 one of our founding associations conducted the largest study to date looking at the presence of personally identifiable information on electronic devices sold on the second-hand market. The study found that 40% of devices resold through publicly-available channels contained personal information.

To ensure credibility, the study was conducted by a third-party forensics lab. Alarmingly, however, the investigation used only basic recovery methods, not sophisticated forensic examination – meaning the information obtained would be accessible to just about anyone. Among the information recovered was credit card information, contact information, usernames and passwords, company and personal data, and tax details. The devices examined included mobile phones, tablets and hard drives.

i-SIGMA feels this study shows the importance of a) ensuring that individuals and organizations take steps to ensure personal information is wiped from their devices before disposing of them on the resale or recycle market, and b) that companies working in electronics recycling and/or resale abide by industry standards for the proper erasure of data.

We believe these findings may have also identified a less thought about route to commit cyber crime and potentially to launch cyber attacks. This risk is only likely to increase with more electronic devices in circulation, which also means more devices eventually

[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/
[5] See https://www.cnbc.com/2023/11/16/morgan-stanley-fined-over-computers-with-personal-data.html

get sent for recycling or destruction. To be blunt, you don't need a sophisticated hacker to bring down a system if instead that person can simply get all the information he needs from an old computer, tablet, phone, etc.

Furthermore, this is a threat that exists for both individuals and companies. While large organizations probably have strong systems in place to ensure discarded electronic devices are cleansed of data, that may not be the case for smaller businesses. Cyber criminals will often target the weakest link in the system, and that could well be the discarded devices of small businesses found on the second hand market (or sometimes just left on the curb).

As it pertains to PIPA, this is one area that would benefit from a requirement to have privacy management programs in place. That would force organizations to think about how they will dispose of old electronics. This is an area of cybersecurity protection that all individuals, businesses and organizations will have to keep in mind as more electronic devices enter the market – and then exit the market at the end of their lifecycle. And as our organization has said for decades: information is only as secure as the weakest link in its lifecycle, and too often little attention is paid to the end of that lifecycle.

To reinforce that point, consider the lifecycle of a paper document containing critical financial, security or personal information. An organization should have protections in place throughout its lifecycle, such as safe storage; clear policies on retention requirements; and then safe destruction and disposal when that information is no longer needed. When it reaches the latter stage, you would not toss it into the trash or recycling bin because it contains valuable information that could be stolen. If someone did dispose of it carelessly in such a manner, all efforts to protect that information during the useful phase of its lifecycle would be negated. That is why attention needs to be paid to the end of the lifecycle; it is just as important as the other phases.

Now consider that same document if it only ever exists in electronic form. People are familiar with protecting their passwords and locking devices, but do smaller businesses know what do to with old electronics? This is a sophisticated area of information destruction and do-it-yourself attempts to cleanse devices are often insufficient, with the information still vulnerable to recapture. As such, when discarding electronics, individuals and organizations may be doing the equivalent of putting a box of critical financial or security information on the curb.

Training

Training is critical, and we recognize that newer aspects of privacy protection are complex, particularly when it comes to electronic devices and records. Therefore, i-SIGMA is always willing to partner with governments and the business community, particularly SMEs, to help their employees develop best-in-class privacy practices. Our members are also in the community every day helping SMEs understand their privacy obligations and could be a conduit for sharing such information.

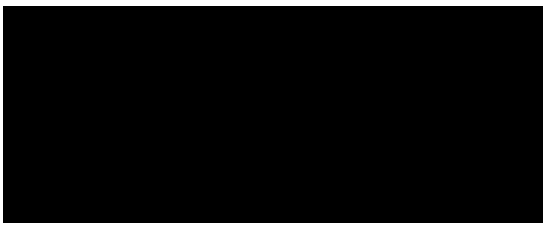
To put that another way: the Government's work is not done if and when PIPA is amended. The effort must then shift to helping organizations comply and giving them the tools to do so. We are ready and able to help in that regard.

Conclusion

We appreciate the opportunity to comment on Alberta's PIPA review and hope that your legislative process moves at a faster pace than the proposed federal changes in Bill C-27. As that process drags on at a glacial pace, Alberta can fill the void and solidify its leadership on privacy protection by updating PIPA.

Thank you for your time and consideration, and please do not hesitate to contact me if you have questions about this submission.

Sincerely,



Tony Perrotta
Director, Canada, i-SIGMA
www.isigmaonline.org