i-SIGMA™

Home of NAID & PRISM International

September 8, 2026

Access to Information and Protection of Privacy Act Statutory Review 2025
2nd Floor, Beothuck Building
20 Crosbie Place
St. John's, NL
A1B 3Y8

Dear Review Committee:

On behalf of the International Secure Information Governance and Management Association (i-SIGMA), thank you for the opportunity to provide comments on the review of the *Access to Information and Protection of Privacy Act, 2025*.

The comments provided in the attached submission are focused on the legislative framework. I wish to add two additional points around implementation.

First, please consider i-SIGMA a resource throughout this process. We believe employee training is critical to privacy protection. As such, we are happy to share our expertise on physical records and information storage, data protection and media vaulting, digitizing and scanning, and confidential records and information destruction services if you are conducting any training sessions.

We also offer a program to become a Certified Secure Destruction Specialist®. This involves study, passing of an intensive exam, and keeping up-to-date on subject matter by earning Continuous Education Units. This may be useful to Chief Privacy Officers.

Second, for public sector entities that outsource any of the information management activities listed above, we recommend the Government mandate they use companies that meet i-SIGMA's NAID AAA Certification.™ Many national and subnational governments do so. Our program is a widely recognized operational standard, particularly because it relies on independent, neutral third-party auditors to verify compliance. It would eliminate the risk of public sector entities trying to assess which external suppliers are best placed to carry out these tasks.

Please do note hesitate to contact me if you have any questions about our submission.

Sincerely,

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

Comments on the Review of the *Access to Information and Protection of Privacy Act, 2015* (ATIPPA)

Policy thesis: A durable provincial privacy law should set enforceable outcomes, align legal duties with operational control, and require measurable lifecycle safeguards without prescribing technologies that the Government cannot future-proof.

Submitted by	International Secure Information Governance & Management Association (i-SIGMA)
Subject	ATIPPA
Purpose	To strengthen the Act through operationally durable, technology-neutral, independently verifiable information governance principles.

Executive Summary

i-SIGMA's previous engagement in Newfoundland and Labrador was through one of our predecessor organizations, the National Association for Information Destruction – Canada (NAID-Canada). NAID-Canada's primary goal was to ensure privacy legislation adequately addresses the need for secure information destruction when personal information is no longer needed. ATIPPA is strong in this regard and incorporates in Section 64(2) almost exactly the definition NAID-Canada has established as the gold standard for destruction.

Our comments for this review will focus at a higher level and address trends and dynamics our association is witnessing as privacy legislation evolves within Canada and internationally.

The central legislative challenge is how the Province can update its framework so that it remains enforceable as information moves across physical records, enterprise systems, cloud services, mobile devices, artificial intelligence environments, and data-bearing equipment. The Government should prioritize a single statutory thesis: privacy rights become meaningful only when legal responsibility follows operational control and when safeguards cover the full information lifecycle.

ATIPPA is a good piece of legislation already, but it will be stronger if the statutory text consistently connects privacy rights to implementable controls. The Province should therefore clarify that compliance is measured by demonstrable practices, not by aspirational policies alone.

i-SIGMA's perspective is practical. Its members support information governance, records management, secure transportation, media protection, digitization, secure destruction of records, data sanitization, and information technology asset disposition across regulated sectors. That experience shows that data risk rarely appears at only one point in an information system. It accumulates when records are retained longer than necessary, media is not tracked, vendors receive unclear instructions, contracts fail to allocate duties, or disposition is treated as an afterthought. The Province should recognize that lifecycle governance is not ancillary to privacy; it is the operating system through which privacy rights are delivered.

Based on its experience in Canada and internationally, i-SIGMA offers five drafting principles for the Committee's consideration as it reviews ATIPPA: align responsibility with decision-making authority; protect information throughout its lifecycle; establish outcomes rather than prescribe technologies; encourage measurable and independently verifiable safeguards; and reinforce trusted information infrastructure. The Committee should use these principles to make ATIPPA durable, technology-neutral, and administrable across the government departments and agencies covered by the legislation.

About i-SIGMA and the Operational Perspective

i-SIGMA is a global trade association representing organizations responsible for secure information management throughout the lifecycle of records, data, media, equipment, and related information assets. Formed through the merger of the National Association for Information Destruction (NAID) and PRISM International, i-SIGMA brings decades of experience at the point where privacy, cybersecurity, records management, vendor oversight, and secure disposition converge.

i-SIGMA members serve organizations in healthcare, financial services, government, legal services, critical infrastructure, technology, education, and other highly regulated markets. Their work includes chain-of-custody controls, secure records storage, scanning and digitization, media protection, secure shredding, data sanitization, device processing, and IT asset disposition. These functions are not peripheral services; they are often the controls that determine whether personal data is retained, transferred, reused, destroyed, or exposed. It is critical to ensure that statutory obligations reach the practical handoffs where privacy risks become real.

That perspective is especially important for legislation that distinguishes among controllers, processors, data brokers, and other covered actors. Those distinctions can improve accountability only if duties correspond to the actor's actual authority over purpose, means, custody, and disposition. A company that decides why data is processed should not be treated the same as a service provider that follows documented instructions; likewise, a processor that independently determines new purposes should not avoid controller duties. Legislation should maintain role-based accountability while making clear that operational control carries legal consequences.

Legislative Context

As noted above, i-SIGMA was created through the merger of NAID and PRISM International. Previous engagement in Newfoundland and Labrador was through NAID-Canada, which was primarily focused on issues around the safe destruction of personal information that is no longer needed.

For years, NAID-Canada advocated for federal and provincial privacy legislation to include both a specific destruction requirement and a definition of destruction. ATIPPA is sound in both regards.

First, it includes a requirement for destruction with Section 64.1(c), which states *"the head of a public body shall take steps that are reasonable in the circumstances to ensure that records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner."* Issues regarding custody and control will be addressed in later sections, but it is positive that a destruction/disposal requirement is included.

Second, NAID-Canada defined 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."* As such, ATIPPA is very closely aligned with that definition with Section 64.2, which states *"disposed of in a secure manner … does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances."*

Therefore, ATIPPA contains the basic elements that i-SIGMA considers critical when it comes to the lifecycle of personal information. With that in mind, the rest of this submission will focus on broader principles that the Committee should consider as it reviews the legislation.

Principle 1: Align Responsibility with Decision-Making Authority

Statutory responsibility should be attached to the entity that determines the purpose, means, custody, or disposition of personal data, and each covered actor should be accountable for the controls within its practical authority. This is needed to prevent both over-assignment and under-assignment of privacy duties.

Role clarity is central to administrability. Legislation should recognize controllers and processors and provide that the determination of role depends on the context in which personal data is processed. That fact-based approach is essential because modern information environments rely on layered service providers, subcontractors, cloud platforms, data managers, disposition vendors, and records custodians. A rigid label-based assignment could impose obligations on entities that cannot perform them or allow entities with real decisional control to evade responsibility. Contextual role analysis is needed when emphasizing documented allocation of duties.

Legislation should also make clear that contracts are not a substitute for accountability. Processor agreements are necessary because they define instructions, confidentiality, deletion or return obligations, assessment rights, subcontractor flow-downs, and assistance with security duties. But contract terms should reflect operational reality, including who can authenticate requests, locate records, suspend deletion holds, return media, destroy physical files, sanitize equipment, or verify completion. Legislation should favour language that requires contracts to map legal duties onto operational capacity.

This approach benefits both consumers and covered entities. Consumers receive clearer accountability when they exercise rights, regulators receive a more reliable compliance trail, and organizations avoid duplicative or conflicting obligations. The result is not weaker regulation; it is enforceable regulation directed at the party best positioned to act.

The Committee should reflect on whether ATIPPA mandates that responsibility follows control, control is documented, and undocumented control does not become a means of avoiding duty. It is not apparent from our reading that it does.

Principle 2: Protect Information Throughout Its Lifecycle

Privacy protection must extend from collection through use, access, transfer, retention, archival storage, and secure disposition, because a failure at any lifecycle stage can defeat consumer rights and data security. Lifecycle governance should be a core feature of any privacy legislation and, as per the earlier section, ATIPPA has a solid foundation in this regard. It also establishes the limited basis on which personal information can be collected.

However, data minimization is not complete when collection is limited; it must also govern retention and disposition. ATIPPA addresses disposition, but lacks a specific directive on retention. Problems arise when covered entities retain obsolete data, duplicate records, unmanaged backups, unneeded physical files, unsanitized devices, or media inventories that no longer serve a lawful purpose. Legislation should

clarify that minimizing data includes minimizing unnecessary retention and requiring defensible disposition.

Secure disposition is a privacy safeguard, a cybersecurity control, and a consumer trust measure. Physical records can expose personal data no less than digital systems; retired laptops, drives, mobile devices, servers, tapes, and other media can retain sensitive data after their business use ends. Secure destruction and data sanitization reduce attack surface, lower breach severity, support deletion rights, and improve the integrity of downstream reuse or recycling. The Province should recognize secure disposition as an operational control that materially advances the Act's privacy and security objectives.

Lifecyle drafting also improves enforcement. Regulators can assess whether an organization knows where personal data resides, who has custody, how it moves, how long it is retained, who may subcontract for it, and how disposition is verified. These are observable practices, not abstractions. The Province should direct attention to verifiable lifecycle controls because privacy rights cannot be reliably honoured for data an organization cannot locate, govern, or retire.

Principle 3: Establish Outcomes Rather Than Prescribe Technologies

A privacy law should prescribe required outcomes and risk-based safeguards, not specific technologies, because statutory text must remain effective after today's systems, platforms, and processing models change.

Technology-neutral drafting is essential when data processing changes faster than legislation. Language should be outcome-oriented. For privacy and information governance, those outcomes include accurate rights response, accountable role allocation, reasonable security, limited retention, documented transfers, auditable processor oversight, secure deletion or return, reliable deidentification practices, and verified disposition. These outcomes allow innovation while preserving enforceability. The Province should describe compliance in terms of demonstrable results that regulators and affected parties can evaluate.

Principle 4: Encourage Measurable and Independently Verifiable Safeguards

ATIPPA requires privacy impact assessments, but written policies should be supported by measurable controls, qualified assessment, recognized standards, and reliable evidence of implementation. The Information and Privacy Commissioner should use the audit powers in ATIPPA so compliance can be tested rather than assumed.

There is also value in recognizing codes of conduct, relevant certifications, third-party attestation, technical specifications, and risk management frameworks in the security context. Those mechanisms can help convert broad statutory duties into practical evidence of compliance. They also create a disciplined way to distinguish organizations that merely describe safeguards from those that implement and verify them.

Also, independent verification is particularly valuable in the vendor ecosystem. Date controllers frequently rely on processors and subcontractors to handle storage, transfer, scanning, destruction, sanitization, or device processing. A contractual promise may be necessary, but it is not always sufficient to establish that the control operates in practice. Assessment rights, qualified independent assessments, written reports, chain-of-custody records, certificates of destruction, sanitization

documentation, and audit-ready evidence create a stronger compliance record. The Province should encourage verification where personal data leaves direct controller custody.

Finally, verification supports regulatory efficiency. Oversight bodies can better focus enforcement when recognized codes, attestations, and control evidence provide a baseline for evaluation.

Principle 5: Reinforce Trusted Information Infrastructure

Privacy, cybersecurity, artificial intelligence governance, records management, and trusted digital infrastructure depend on the same foundation: knowing what information exists, where it resides, who controls it, how it is protected, and when it should be securely retired.

Privacy is now inseparable from broader information infrastructure. Personal data is used in customer systems, employment systems, analytics, artificial intelligence tools, identity services, vendor platforms, archives, physical records, and devices moving through repair, resale, recycling, or destruction. Weak governance in any of those channels can create privacy harm, cybersecurity exposure, operational disruption, or public distrust. The Province should make clear that trusted infrastructure requires both digital and physical information controls.

From Theory to Practice

Please allow us to put all the above into practical, real-life examples.

In 2010, NAID-Canada (one of i-SIGMA's predecessor associations) 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. That exercise has been repeated in Australia and Spain and sparked national conversations around the failure to securely destroy information that is no longer needed.

In 2017, NAID (US) conducted a study looking at the presence of personally identifiable information on electronic devices sold on the second-hand market. It found that 40% of devices resold through publicly-available channels contained personal information, including 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 and the recovery methods used were basic, meaning this information would be accessible to just about anyone.

More than a decade later, the problem seemingly persists. For example, on January 13, 2026, the Privacy Commissioner of Canada released the results of an audit that found Staples Canada continues to face challenges ensuring returned laptops then resold are cleansed of personal information. This came 15 years after the Commissioner initially flagged this issue at Staples.[1]

Furthermore, the public sector is not immune to this challenge. In 2010, an audit conducted by the Privacy Commissioner of Canada found that Federal Government computers being donated to the Computers for Schools program had an alarming amount of sensitive personal data retained on them.[2]

These examples highlight several important factors that the Province must keep in mind.

[1] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260113/
[2] https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_pidp_2010/

First, generally speaking, there are destruction requirements in the jurisdictions covered in the studies above. That demonstrates that just having a law is not enough. Employees must understand it and be trained on compliance.

Second, regulators and/or privacy authorities must conduct regular inspections or audits to ensure statutory obligations are being adhered to. This is critical to identifying potentially systemic problems.

Third, who was responsible for the unsafe destruction in the examples above? If a contract mandated safe destruction and the contractor failed to comply, then fault lies with the latter. However, if the data controller did not provide clear instruction to the contractor, then fault should lie with the data controller. In either case, the key question is whether the legislation would appropriately assign that responsibility and accountability.

Finally, the study on electronic devices demonstrates a perhaps unconsidered cybersecurity risk. You do not need a sophisticated hacking operation if instead criminals can simply gain access to critical systems by picking up some old computers that have not been property cleansed of critical information. This reinforces the fact that all the issues – privacy, cybersecurity, chain of custody, lifecycle management – are interrelated.

Summary and Conclusion

i-SIGMA encourages the Committee to reflect on the following key points:

- Does ATIPPA mandate that responsibility follows control, control is documented, and undocumented control does not become a means of avoiding duty?
- Does ATIPPA ensure that controller-processor contracts address lifecycle responsibilities, including custody, transfer, subcontracting, return, deletion, destruction, sanitization, and records sufficient to demonstrate completion?
- Does ATIPPA clearly define retention schedules?
- Is ATIPPA technology-neutral?
- Does ATIPPA allow flexible paths for recognized codes of conduct, certifications, third-party attestations, and risk management frameworks, while making clear that such evidence is not a shield for material noncompliance?
- Are audit powers for the Information and Privacy Commissioner strong enough, and are they being used sufficiently to verify compliance?
- Do government employees understand their obligations under ATIPPA and how is the government measuring that?

To reiterate, i-SIGMA believes privacy legislation should be built around five principles: responsibility should follow decision-making authority; personal data should be protected throughout its lifecycle; the statute should require outcomes rather than prescribe technologies; safeguards should be measurable and independently verifiable; and privacy should be treated as part of trusted information infrastructure. These principles make legislation more durable without making it rigid.

Finally, i-SIGMA appreciates the opportunity to comment and would welcome the opportunity to serve as a technical resource. Our members operate at the practical points where information is collected, stored, transferred, retained, digitized, destroyed, sanitized, and retired. That operational vantage point can help ensure ATIPPA is not merely well drafted, but capable of being implemented across the government.