Centre for International
Governance Innovation

CIGI Papers No. 281 — September 2023

Enhancing Compliance with Privacy Legislation through Standardization

Michel Girard

Centre for International
Governance Innovation

CIGI Papers No. 281 — September 2023

Enhancing Compliance with Privacy Legislation through Standardization

Michel Girard

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Director, Program Management Dianna English
Project Manager Jenny Thiel
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Abhilasha Dewan

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Michel Girard is a senior fellow at CIGI, where he contributes expertise in the area of standards for big data and artificial intelligence (AI). His research strives to drive dialogue on what standards are, why they matter in these emerging sectors of the economy, and how to incorporate them into regulatory and procurement frameworks. He highlights issues that should be examined in the design of new technical standards governing big data and AI in order to spur innovation while also respecting privacy, security and ethical considerations.

In addition, Michel provides standardization advice to help innovative companies in their efforts to access international markets. He contributes to the Digital Governance Council and to the standardization activities of the Digital Governance Standards Institute.

Michel has 22 years of experience as an executive in the public and not-for-profit sectors. Prior to joining CIGI, Michel was vice president, strategy at the Standards Council of Canada (SCC), where he worked from 2009 to 2018. At SCC, he led the design and implementation of the Standards and Innovation program, the Climate Ready infrastructure program, the Northern Infrastructure Standards Initiative and the Monitoring Standards in Canadian Regulations project. He managed the negotiation of standardization clauses in trade agreements including the Comprehensive Economic and Trade Agreement and the Canadian Free Trade Agreement. Previously, he was director of the Ottawa office at the Canadian Standards Association, director of international affairs at Environment Canada, corporate secretary at Agriculture Canada and acting director of education and compliance at the Canadian Environmental Assessment Agency. He holds a Ph.D. and a master's degree in history from the University of Ottawa.

Acronyms and Abbreviations

ACI	Association of Chief Boiler and Pressure Vessel Inspectors
AHJs	authorities having jurisdiction
AHRI	Air-Conditioning, Heating, and Refrigeration Institute
AI	artificial intelligence
ASABE	American Society of Agricultural and Biological Engineers
ASME	American Society of Mechanical Engineers
BNQ	Bureau de normalisation du Québec
CAC-GDPR	Canadian Advisory Committee on the General Data Protection Regulation
CACES	Canadian Advisory Council on Electrical Safety
CACP	Canadian Advisory Council on Plumbing
CBHCC	Canadian Board for Harmonized Construction Codes
CCBFC	Canadian Commission on Building and Fire Codes
CEC	Canadian Electrical Code
CETA	Canada-European Union Comprehensive Economic and Trade Agreement
CGSB	Canadian General Standards Board
CSA	Canadian Standards Association
DGSI	Digital Governance Standards Institute
EA	European Accreditation
ETSI	European Technology Standards Institute
FPT	federal/provincial/territorial
GDPR	General Data Protection Regulation

HRSO	Human Research Standards Organization
HSO	Health Standards Organization
IAPMO	International Association of Plumbing and Mechanical Officials
ICT	information and communications technology
IEC	International Electrotechnical Commission
IEEE SA	Institute of Electrical and Electronics Engineers Standards Association
IoT	Internet of Things
IP	intellectual property
ISED	Industry, Science and Economic Development
ISMS	information security management system
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
JTC	Joint Technical Committee
MOU	memorandum of understanding
NPSAC	National Public Safety Advisory Committee
NRC	National Research Council Canada
NSC	National Standard of Canada
PII	personally identifiable information
PIPEDA	Personal Information Protection and Electronic Documents Act
P/T	provincial/territorial
PTAC	Provincial-Territorial Advisory Committee
RAAB	Regulatory Authority Advisory Body
SCC	Standards Council of Canada
SDOs	standards development organizations
SDOAC	Standards Development Organizations Advisory Committee
TBT	technical barriers to trade
UL	Underwriters Laboratories
ULC	Underwriters Laboratories of Canada
WGs	working groups
WTO	World Trade Organization

Executive Summary

Although privacy legislation can apply to any organization in Canada, regulators are not currently organized to guide the development and implementation of broad-based standards and compliance programs. This paper proposes an approach whereby privacy commissioners can directly engage with standardization and professional bodies without jeopardizing their neutrality and independence. It borrows from approaches that have been set up by federal/provincial/territorial (FPT) regulators accountable for the health, safety and security of consumer products, devices, processes and infrastructure.

By creating a privacy Regulatory Authority Advisory Body (RAAB), regulators can set standardization priorities and ensure that new compliance programs meet regulatory objectives. This can be achieved without amending legislation. Once the desired standards and compliance programs are developed and reviewed, individual regulators can make a final decision regarding their adoption. Approved documents can be referenced in regulations or added to lists of recognized standards.

Introduction

As Canadian organizations accelerate the pace of digital transformation, complying with privacy legislation has become a critical success factor. Provincial and federal governments are slated to introduce new privacy legislation enabling customers to make specific requests regarding the use and exchange of personal information.[1] Firms doing business in Europe must also comply with the General Data Protection Regulation (GDPR).[2] In response, organizations need to put in place systems to manage a wide range of privacy requests. Additionally, organizations need to set up credible data comptrollership functions to monitor and report on compliance with privacy legislative requirements.

Mastering compliance with privacy requirements has become a precondition to achieve digital transformation. Without privacy systems and comptrollership functions, organizations simply will not be able to share data efficiently, either internally or with other parties. One needs large quantities of data from various sources to feed algorithms embedded in products and systems, or to pursue advanced analytics. In addition, new platforms and technologies (such as Internet of Things [IoT] devices and wearables used in the rapidly growing telehealth-care and wellness sector) will require ongoing privacy management to keep users safe from harms, as the consequences of breaches can lead to catastrophic outcomes (Fadrique et al. 2020).

Initial data on compliance with the GDPR illustrates the scale of the problem faced by organizations. In 2022, more than 109,000 breaches were reported to European data protection agencies (McKean et al. 2023, 3). The survey only included breaches that were reported to regulators. Fines for the year amounted to €1.64 billion, a 50 percent year-over-year increase compared with 2021 (ibid.).

To support this transition, organizations large and small will be compelled to implement new standards and compliance programs. At the firm level, many standards have already been developed, but gaps exist and should be filled.[3] Additionally, new standards, specifications and testing protocols are required for the high-risk products and devices mentioned above to ensure they are privacy compliant.

It is possible for privacy regulators to get involved in standardization in a formalized way while maintaining their neutrality and independence. They already offer advisory services to help individual organizations understand what needs to be done to comply with legislation. However, there is no mechanism in place to guide the development, adoption and use of broad-based supportive standards and compliance programs. A new advisory body could be created to connect privacy regulators with relevant standardization bodies and with stakeholders.

1 *Digital Charter Implementation Act*, 2022, C-27, 44th Parl, 1st Sess, online: <www.parl.ca/legisinfo/en/bill/44-1/c-27>.

2 See https://gdpr.eu.

3 See www.scc.ca/en/flagships/data-governance.

Some may remember Canadian privacy commissioners' first exposure to standardization activities more than 30 years ago. In the 1990s, representatives from the Ontario and Canada privacy offices engaged with industry stakeholders, experts and consumers through the auspices of the Canadian Standards Association (CSA) and worked on the development of a first generation of privacy standards. In March 1996, following years of deliberations, the CSA Technical Committee on Privacy published the first edition of the Model Code for the Protection of Personal Information. The model code, which was adopted as a National Standard of Canada (NSC), proposed 10 principles to organizations on collecting, using, disclosing and protecting personal information. It also outlined in broad terms the rights of individuals to access personal information about themselves and, if necessary, to have the information corrected.[4] Interestingly, the model code was later incorporated into federal legislation.[5]

This paper proposes to build from that success story. It presents the case that externally developed privacy standards, codes of practice or certification/accreditation systems can offer agile means of supporting the trusted and trustworthy adoption of innovative systems, controls, technologies and platforms, while ensuring privacy safeguards are built into the adopting organization's operations. However, these enabling tools cannot be developed in a vacuum. Stakeholders need privacy regulators at the table to get it right.

Privacy regulators can set up a new governance mechanism to engage with stakeholders and articulate a viewpoint about standardization priorities without jeopardizing their neutrality and independence. In order to achieve that objective, this paper proposes that FPT regulators engage with Canada's standardization system through a privacy RAAB. This body would enable regulators to set standardization priorities; review, adopt or adapt relevant standards; oversee the development and implementation of compliance programs; engage with professional associations with expertise in audit and assurance services; and share information regarding emerging issues that require standardization support. This opens the door for standards development organizations (SDOs) and the Standards Council of Canada (SCC) to recognize privacy regulators as authorities having jurisdiction (AHJs) over relevant privacy standards, technical specifications, safety codes and certification programs.

This approach has been adopted by FPT regulators in a wide range of sectors such as electrical, plumbing, fuels, elevating devices and consumer goods, occupational health and safety, fire safety and energy efficiency as well as infrastructure (European Delegation to Canada 2020). Through this approach, regulators get engaged in standardization while maintaining their independence to perform enforcement activities. It also allows individual jurisdictions to review standards and model codes once developed and make a final determination on their suitability for adoption.

Standards, safety codes and third-party certification by accredited bodies are routinely used by regulators across Canada to meet a wide range of health, safety and security objectives. FPT regulators and chief inspectors routinely meet and engage with SDOs to set standardization priorities, develop and review new standards, assess changes to existing standards and provide guidance on certification programs. Standards are embedded in hundreds of regulations. In 2020, there were 6,073 references to standards and safety codes in FPT regulations, and that number is growing (SCC 2022, 21). Millions of products, devices, components and systems are tested and certified annually through various compliance programs accredited by SCC. From a health, safety and security perspective, the system proved to be effective. Although product recalls are unavoidable, low rates of product defects resulting in accidents, injuries or deaths are reported. Many believe that similar positive compliance outcomes can be achieved for privacy as well.

In order to delineate a sound rationale for the creation of the proposed privacy RAAB, this paper provides substantial background information on the main features of the standardization system internationally and in Canada. The author fully acknowledges that standardization is not a top-of-mind issue for most decision makers and regulators. Moreover, Canada's standardization system is complex. Its features need to be described before one can look at possible governance mechanisms.

4 See www.scc.ca/en/standardsdb/standards/6176.

5 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1, online: <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/>.

The first section provides background information on standards development, certification, assurance and accreditation internationally. This section also describes Canada's standardization system. It explains the role of SCC, accredited SDOs, certification bodies and accreditation bodies. It provides information on the use of standards and safety codes by provincial and federal regulatory entities based on information generated by SCC. It also explains the various ways that standards are referenced as a compliance mechanism.

The second section focuses on the mechanisms that FPT regulators use to engage with Canada's standardization system. It explains how provincial regulators and chief inspectors accountable for health, safety and security in sectors such as electrical, buildings, plumbing or gas have organized themselves into informal advisory councils and regulatory committees.

The third section reports on the state of affairs concerning standards designed to comply with privacy legislation. It starts with lessons learned and standardization activities that have taken place since the publication of the CSA's model code. It then presents the use case for the GDPR and standards that are recommended to enhance compliance.

The conclusion focuses squarely on the creation and operations of a privacy RAAB. It looks at options for a governance model and delineates some of the key activities that a privacy RAAB could undertake to spur the development and adoption of standards and compliance programs.

Background information on what are standards can be found in the annex.[6]

Standardization in Canada

Canada's standardization system shares many features with the international system described in the annex. This section outlines various types of documents, conformity assessment programs as well as key actors engaged in standardization.

Standards, Technical Specifications and Safety Codes

Fundamentally, Canada's standardization produces three types of documents: standards, technical specifications and safety codes. Conformity to standards and technical specifications is managed through conformity assessment bodies accredited by SCC. Conformity to safety codes is managed through field inspectors reporting to chief inspectors or municipal inspectors in each province and territory.

Standards

At the core of Canada's standardization system are voluntary standards. They describe the important features of a product, service or system. Canadian standards are developed through consensus by committees of affected stakeholders that may include representatives from industry, governments, academia and the public interest. Figure 1 showcases the process used for the development of standards under SCC-accredited SDOs.

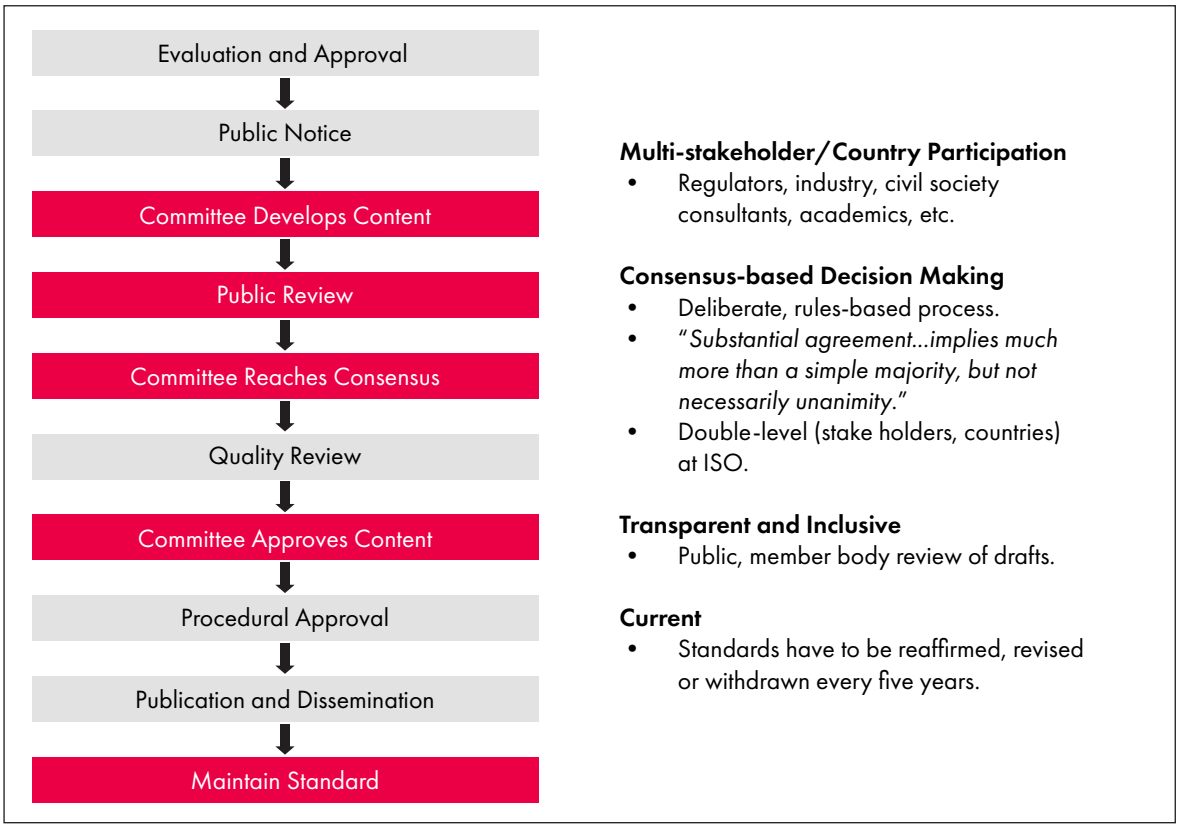
SCC accreditation requirements are fully aligned with accepted international standards best practices. They are mostly derived from annex 3 of the World Trade Organization's (WTO's) technical barriers to trade (TBT) provisions. Additional requirements are taken from the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) (ISO 2019).

SCC's requirements are meant to ensure compliance with the following principles:

- consensus;
- equal access and effective participation by concerned interests;

6 The text in this annex also appears in the paper *Canada Needs Its "New Approach" to Streamline Digital Rulemaking* by Michel Girard (CIGI Paper No. 278).

Figure 1: How Canadian Standards Are Developed



Source: Girard (2019, 6).

- → respect for diverse interests and identification of those who should be afforded access to provide the needed balance of interests;
- → openness and transparency;
- → open access by interested parties to the procedures guiding the standards development process;
- → clarity with respect to the processes;
- → safeguarding Canadian interests as the basis for the development of standards by SDOs;
- → avoiding duplication of standards or overlap with the work of other SDOs or with the work of relevant international or regional SDOs; and
- → adherence to an established mechanism for duplication resolution. (SCC 2019a)

Domestic standards development activities revolve around technical committees managed by an accredited SDO. SCC requires a balanced matrix of interests including industry, regulators, academics/technical experts and consumer representatives. Committee size generally varies from 16 to up to 32 members. The Digital Governance Standards Institute, however, adopted an online collaborative software to support standards development activities. It has seen some committees grow to more than 100 members. However, it must ensure that any committee has appropriate representation from every required stakeholder group.

The first official step in the process is for one accredited SDO to register a new work item in SCC's Central Notification System for approval. The notification must clearly demonstrate that no other international standards already exist, that there is a net benefit for the development of a new standard and that one or many stakeholder groups support the development of a new document.

If an international standard exists, it can be adopted as an NSC through a formal adoption process led by an accredited SDO. Generally, no deviations

are made to international standards, although it is possible for the technical committee to do so.

The second step for the accredited SDO is to create a technical committee, establish the terms of reference for the new work item and nominate a chair from volunteer members. The SDO assigns a secretary to the committee who is responsible for both upholding the process and drafting documents and minutes from the meetings.

The third step is the drafting of the document. Often, stakeholders will submit a "seed document" to launch deliberations by the committee. The committee meets and works its way through the various sections of the standard.

The draft document, once ready, will be made available for public review through the SDO website for a set period. The chair and secretary will then tabulate comments pursuant to various clauses of the standard. The committee must review and dispose of each comment submitted by stakeholders through the public review. Each decision by the committee (to either accept or reject a comment) needs to be documented, which results in a new version of the document being produced.

A final version of the document is then submitted to technical committee members for approval through formal voting and balloting, administered by the secretary and the chair. There are detailed rules regarding approval. For example, there must be at least one approval from each of the stakeholder groups around the table for a standard to be approved. Once approved, the final version of the standard can then be translated. The standard is then submitted by the SDO to SCC for approval as an NSC.

The technical committee is not disbanded following publication. It can be reconvened at any time if significant changes require a revision of the document. It is also invited to reconvene for the five-year review of the document.

Central Notification System

When developing a new standard or updating an existing one, SDOs are required to submit a notice of intent on SCC's Central Notification System. Given limited resources and expertise available in the country, SCC does not permit the development and maintenance of duplicate NSCs, nor the development of domestic standards when international standards can be used. As such, any time an SDO prepares to update an existing standard or develops a new one, it has an obligation to submit a notice of intent on SCC's database. Interested stakeholders have 15 days to declare whether they oppose the notification.

This mechanism allows industry representatives or regulators to declare whether another SDO should be entrusted with the development of a standard. This approach was developed to avoid the creation of virtual "monopolies" by specific SDOs and allow industry and regulators to engage with all relevant SDOs and to choose relevant standards that meet their needs (SCC 2017).

Standards Development Organizations Advisory Committee

When SCC was created in 1970, it constituted a Standards Development Organizations Advisory Committee (SDOAC), composed of the CEOs of its accredited SDOs. The SDOAC is accountable to do the following:

- advise and make recommendations to the council on matters related to voluntary standards development;
- promote cooperation and communication between the council and the SDOs represented on the committee;
- provide a coordinated SDO view to council on matters of voluntary standardization and the National Standards Strategy;
- identify and provide guidance and advice to SCC on emerging issues of standardization; and
- provide feedback to SCC on policies directly affecting SDOs.

The SDOAC's role has evolved with the accreditation of US-based SDOs and Canadian SDOs focusing on emerging sectors. It is overwhelmingly supportive of the timely adoption of standards and safety codes by provincial/territorial (P/T) regulators, is actively looking at ways to increase the accessibility of mandatory standards and safety codes to the public, and is exploring ways to diversify its service offerings to support the rapidly growing information and communications technology (ICT) and digital governance sectors.

Roles of Regulators

Canada does not impose restrictions on the use of specific standards in a given area or field. Although the use of international standards is encouraged, industry and regulators are free to choose the ones they will incorporate in their supply chain contracts or regulations. As indicated above, voluntary standards are used by regulators as a compliance mechanism. Once a voluntary standard has been incorporated by reference in a regulation or a related instrument, it is deemed to be mandatory in that jurisdiction.

Regulators therefore have two roles to play. The first role is associated with the standards development process itself. When a Canadian standard is being developed, if there is an expectation that it will later be referenced in a regulation and become a mandatory standard, a small group of regulators is expected to participate in the deliberations of the technical committee and in the drafting of the document. This is to ensure that the standard meets regulatory objectives. There is also an expectation that regulators who are part of the balanced matrix of interests for the committee should be comfortable enough with the final version of the text of the document to vote in favour of its publication.

As indicated in the section titled "Privacy Standards and Compliance Mechanisms," voting in favour of the publication of a document by a regulator does not imply that it will be automatically adopted in their jurisdiction. That is the second role that regulators will play: bringing the published standard back to their respective jurisdictions to determine whether to either:

- → adopt the standard in the regulation as is;
- → apply deviations to the requirements that can be added in the text of the regulation or to an addendum to the standard; or
- → refrain from adopting the document.

Technical Specifications

In addition to voluntary standards, regulators also adopt technical specifications. The documents can be developed in the absence of a recognized Canadian standard without using the full consensus process normally associated with an NSC. A technical specification may be developed in a field where the technology, or a related aspect such as the regulatory environment, is undergoing rapid change and where speed of delivery, rather than full consensus, is of paramount importance. At a minimum, it is subject to limited peer review with the option of going to full public comment if it is deemed to be warranted (SCC 2019b).

Safety Codes

A defining feature of Canada's standardization system is the use of safety codes by FPT regulators. Codes can be defined as a series of rules and objectives applying to a particular sector. Codes cover a wide range of issues and are developed with the intention of being given the force of law through adoption by a provincial, territorial or municipal authority. In essence, safety codes are detailed draft regulations created by multi-stakeholder committees. They blend the "what" to do and the "how" to achieve compliance. Whereas the requirements are contained in the body of the document, the compliance tools are embedded in annexes featuring lists of approved products and systems standards. Literally thousands of Canadian, US and international standards and technical specifications are appended in annexes pursuant to model codes.

Safety codes cover the areas of accountability of chief inspectors. There is no single governance model to manage the development and maintenance of these codes. Some are maintained by SDOs accredited by SCC. Some are managed by the Canadian Board for Harmonized Construction Codes (CBHCC) (formerly the Canadian Commission on Building and Fire Codes or CCBFC). Others, such as the Elevator Code, are developed through the participation of Canadian chief inspectors in US-based SDOs (in this case, the American Society of Mechanical Engineers [ASME]). Most safety codes are updated every five years. Some, such as the Canadian Electrical Code (CEC), are updated every three years.

It may be possible for a privacy RAAB to guide the development of a new privacy code that binds together objective-based requirements in the body of the text as well as annexes containing approved standards and technical specifications that organizations need to apply for compliance purposes.

Certification and Accreditation

Third-party certification of products and systems has been a cornerstone of Canada's health and safety framework for decades. It is based on accreditation programs managed by SCC.

Certification

Third-party certification involves contracts between manufacturers and accredited certification bodies whereby prototypes and samples collected during production are tested against specific standards. Regulators are not involved in the product's certification process and do not retest certified products to verify compliance unless systematic defects are reported by consumers.

Once tested by certification bodies, compliant products will bear appropriate certification marks. Products that do not bear appropriate marks are removed from store shelves through regular visits of retail stores by field inspectors reporting to chief inspectors. Most consumer products, infrastructure components and health and safety equipment are standardized and require third-party certification to demonstrate mandatory compliance with health and safety regulations. Up until the ratification of Canada's free trade agreement with the United States in the 1980s, only two certification bodies were responsible for the certification of consumer products in Canada: the CSA and Underwriters Laboratories of Canada (ULC). Since then, the number of certification bodies accredited by SCC has been growing significantly.

Certification marks also bear specific identification numbers referring to the relevant standard used for testing the product. Certification bodies maintain comprehensive lists of certification marks and related standards on their websites, and these are constantly adjusted to match provincial requirements.

Canadian regulators and chief inspectors are overwhelmingly supportive of third-party certification by accredited bodies to manage the safety of consumer and infrastructure-related products.

Regarding management system standards, such as the ISO 9000 series focusing on quality or the 31000 series focusing on risk management, registration and certification are conducted through audits by certified professionals, often through large auditing firms.

Accreditation

SCC manages 10 accreditation programs, which oversee conformity assessment activities. Most are based on ISO and IEC accreditation standards:

- management systems certification bodies;
- product, process and service certification bodies;
- inspection bodies;
- greenhouse gas validation/verification bodies;
- bodies performing the certification of persons;
- SDOs;
- testing and calibration laboratories;
- medical testing laboratories;
- proficiency testing providers; and
- good laboratory practices facilities.[7]

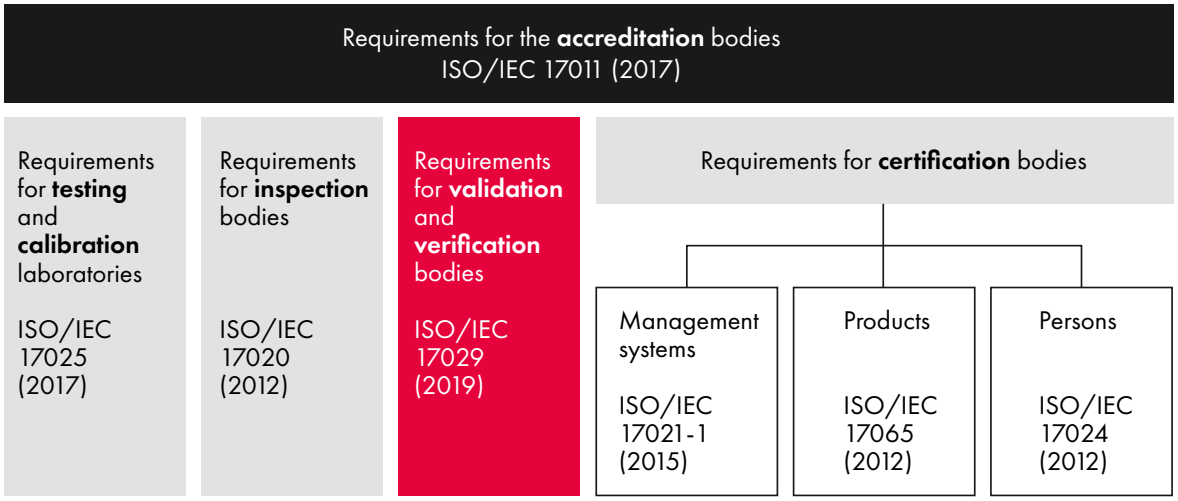
Looking forward, a new ISO accreditation standard has been published to facilitate third-party verification and validation of digital governance standards by professional classes including chartered professions. This recent development could have a profound impact on the development of new privacy standards, codes of practice and compliance programs. The ISO 17029 accreditation standard titled "Conformity assessment — General principles and requirements for validation and verification bodies" sets the stage for claims by organizations adhering to new digital governance standards to be validated and verified through assurance engagements.

As Figure 2 shows, ISO 17029 is complementary to other ISO accreditation standards. It avoids duplication by focusing on activities not covered by the other 17000 series standards. Activities including industrial automation systems, software and systems engineering, artificial intelligence (AI), information technology (IT), privacy management standards or codes of practice may fall under this standard.

ISO 17029 opens the door for a wider range of organizations to develop compliance programs such as by industry bodies and trade associations that decide to become a program owner. Program

7 See www.scc.ca/en/accreditation.

Figure 2: ISO/IEC Accreditation Standards



Source: Committee on Conformity Assessment (2019, 7).

owners are defined as responsible for developing and maintaining specific validation/verification programs focused on conformity to individual standards. ISO 17029 defines a validation/verification program as a set of rules, procedures and management for carrying out validation/verification activities in a specific sector or field, specifying the scope of validation/verification, competence criteria, process steps, evidence-gathering activities and reporting. Privacy codes of practice developed by industry associations could therefore be managed under this new standard.

The release of ISO 17029 in 2019 represented a watershed moment in the international conformity assessment ecosystem because it formally opened the door to professional classes, such as chartered accountants, engineers or auditors, to perform conformity assessment work against digital governance standards.

It becomes possible to adapt the practice of "assurance as a service" as a platform to perform validation and verification services against digital governance standards and codes of practice. Assurance as a service enables people to assess whether systems are trustworthy. It originates from the accounting profession and is used by chartered professionals to cover many domains, such as quality management and cybersecurity, using requirements embedded in international standards to verify and validate claims. Assurance as a service is based on five principles:

- a three-party relationship (composed of a responsible party, a practitioner and an assurance user);
- agreed and appropriate subject matter (the information can be subjected to procedures for gathering sufficient and appropriate evidence);
- suitable criteria (required for the consistent measurement and evaluation of the subject matter within the context of professional judgment);
- sufficient and appropriate evidence (sufficiency relates to the quantity of evidence whereas appropriateness relates to the quality of the evidence, its relevance and reliability); and
- conclusions (the assurance obtained about the subject matter information). (Centre for Data Ethics and Innovation 2021)

Comprehensive Economic and Trade Agreement Conformity Assessment Protocol

As mentioned above, SCC also administers the implementation of the Conformity Assessment Protocol under the Canada-European Union Comprehensive Economic and Trade Agreement (CETA). The protocol is expected to facilitate trade for businesses in Canada and in Europe. Under the protocol, SCC and EA (European Accreditation) are building mutual recognition of accreditation programs and assessments. When

fully implemented, laboratories located in Canada will be able to perform tests on Canadian products using relevant EU standards in order to certify that they meet European requirements before being shipped and vice versa. This process will eliminate the need for duplicative testing and certification. Looking forward, formal mutual recognition of Canadian and European privacy standards could be envisaged through this mechanism.

Key Players in Canada's Standardization System

SCC

SCC is a federal Crown corporation reporting to the minister of Industry, Science and Economic Development (ISED). It was established in 1970 to coordinate Canadian participation in international standardization activities, manage Canadian accredited SDOs and respond to national standardization priorities. A Provincial-Territorial Advisory Committee (PTAC) was created to seek input from provincial and territorial governments. Both SCC's council and PTAC were entrusted to set comprehensive Canadian standardization strategies for key sectors of the economy nationally, regionally and internationally.

SCC's Standards and International Relations Branch is responsible for the accreditation of SDOs, the approval of NSCs, the management of participants and mirror committees at ISO and IEC, and the interface with other standards bodies through bilateral arrangements or through participation in regional standardization bodies. SCC's participation in multilateral accreditation agreements allows for the mutual recognition of accreditation programs around the world. They are the base from which a jurisdiction can recognize test results from laboratories located outside of its jurisdiction, thereby avoiding the obligation to perform multiple duplicative testing for a specific product.

SCC also maintains bilateral agreements with other standardization bodies to facilitate a dialogue and resolution of bilateral standardization issues.

Since 2010, SCC began its involvement in trade and innovation policy through the creation of a Policy Branch, which later became the Strategy and Stakeholder Engagement Branch. It focuses on three key deliverables: the development of Canadian positions and supportive clauses for standards and conformity assessment chapters in bilateral and multilateral trade agreements; the alignment of standards and safety codes incorporated by reference in FPT regulations to reduce internal barriers to trade; and the development of strategies to help Canadian innovative companies become standards makers internationally.

SCC's Accreditation Branch manages its accreditation programs listed in the previous section and provides services to more than 600 customers.

In 2021, SCC had a staff of 149 (SCC 2022, 4) and a total budget of $29.5 million. SCC's total revenues were $10.4 million (ibid., 29). Its federal governmental appropriation totalled approximately $19.3 million (ibid., 31).

Accredited SDOs

As mentioned earlier in the paper, SCC began its operations in 1970 with four Canada-based accredited SDOs. Starting in 2012, it began to accredit US-based SDOs in order to reflect the growing use of US standards by industry and in safety codes and FPT regulations. The initial four SDOs accredited by SCC following its creation in 1970 are presented first. SDOs accredited by SCC in a second phase starting in 2012 are then presented with a short synopsis of standards under development.

- **CSA:** CSA was created in 1919 in Ottawa to adopt, adapt and develop standards supporting Canada's industrialization. It developed new standards, testing and product certification programs across sectors, starting with railways, electrical, plumbing and gas, then branching out to other industrial and infrastructure sectors. CSA assists regulators and chief inspectors in developing safety codes covering electrical, gas, elevators and bridges. CSA Group is a globally active organization with testing and certification operations in North America, North and Southeast Asia, China, Europe and India. Regarding its standards development division, membership now stands at 10,600 members, a significant growth over the 7,500 members registered in 2009. In 2021, it published 572 documents, including 134 new standards (CSA Group 2022, 8).
- **ULC:** ULC is an independent product safety testing, certification and inspection organization. It was created in the 1920s to support the need

for fire protection standards. Since then, it has expanded its range of services to building and construction materials, building envelope performance and environmental performance standards in addition to fire suppression, fuel-burning and distribution equipment. It provides ongoing support to the Council of Canadian Fire Marshals and Fire Commissioners.

- **Canadian General Standards Board (CGSB):** CGSB is a standards development body created in 1934 by the Government of Canada. It reports to the federal department of Public Works and Government Services Canada and developed standards to support the Government of Canada and the military in their procurement activities.
- **Bureau de normalisation du Québec (BNQ):** BNQ was created in 1961 by the Quebec government. In addition to traditional areas such as concrete structures and construction materials, it focuses on emerging sectors such as 3D printing, hydrogen, sustainable responsible management of public events and sustainable horticulture practices.
- **ASTM International:** ASTM International was created as the American Society for Testing and Materials in 1898. It maintains more than 13,000 standards covering a wide array of sectors. It received SCC accreditation in 2013. ASTM International has more than 30,000 members across 140 countries. More than 1,400 Canadians are participating in ASTM International committee work.
- **Underwriters Laboratories (UL):** UL was created in 1894. Its standards catalogue is more than 1,700 documents. UL has more than 14,000 employees and operates in 140 countries. It received SCC accreditation in 2013.
- **Air-Conditioning, Heating, and Refrigeration Institute (AHRI):** AHRI is a North American trade association representing more than 300 Canadian and US manufacturers of air conditioning, heating and commercial refrigeration equipment.
- **NSF:** NSF was founded as the National Sanitation Foundation in 1944 to protect and improve global human health. NSF facilitates the development of public health standards and certifications that help protect food, water, consumer products and the environment.
- **Health Standards Organization (HSO):** HSO is a Canadian SDO focusing on standards for the health-care sector. It was accredited as an SDO in 2017. The parent organization, Accreditation Canada, is also accredited by SCC as a conformity assessment body. HSO has developed more than 100 standards related to the health-care and social services sectors.
- **Digital Governance Standards Institute (DGSI):** Members of the CIO Strategy Council created the Digital Governance Council and DGSI in 2023. Its work program includes more than 35 new work items in areas such as AI systems, cybersecurity, digital identity and credentials, biometrics, data governance in the health-care sector, electoral voting technologies as well as privacy and access control.
- **International Association of Plumbing and Mechanical Officials (IAPMO):** IAPMO is a large US-based standards and certification body. It manages uniform codes for plumbing, mechanical and solar as well as swimming pools.
- **Human Research Standards Organization (HRSO):** HRSO is a not-for-profit Canadian organization that focuses on human research. It received its SCC accreditation in 2020 and focuses on topics such as the development of human research protection programs, ethical issues and conducting research during publicly declared emergencies.
- **Accessibility Standards Canada:** Accessibility Standards Canada creates accessibility standards for federally regulated entities and federal organizations. It is working on 11 standards covering topics such as the built environment, signage, employment and emergency measures.
- **American Society of Agricultural and Biological Engineers (ASABE):** Accredited in 2023, ASABE maintains more than 100 standards in the fields of agricultural equipment and machinery.

CBHCC

Another important component of Canada's standardization system is the new CBHCC. As noted earlier, responsibility for building regulations in Canada rests with the provinces and territories and resulted in a multiplicity of regulations being developed over time as each province and

municipality tried to deal with its own needs. In 1937, the federal Department of Finance asked the National Research Council Canada (NRC) to develop a model building regulation that could be adopted by all municipalities in Canada. The result of that initiative was the publication of the first edition of the National Building Code in 1941.

In order to fully involve provinces and other stakeholders in the development and maintenance of codes, the NRC and provinces created the CCBFC, a decision-making body that provided direction and oversight on the development of the building, fire, plumbing, farm building and energy codes, and encouraged uniformity of building and facility regulations throughout Canada. A new edition of the codes is issued every five years. Each code contains lists of mandatory standards focused on the performance of individual components and equipment. Once codes are approved, provinces and territories are responsible for managing their adoption into regulations. Most jurisdictions undertake individual regulatory impact analysis statements, which require a review of each amendment to assess the costs and benefits associated with its introduction.

In 2022, a new governance model for the construction codes development system was established and a CBHCC was set up (see more information in the section titled "Privacy Standards and Compliance Mechanisms").

Policy Advisory Committees

Two federal agencies share the bulk of the work to orchestrate pan-Canadian coordination and liaison efforts: SCC and the NRC. The two organizations report to the federal minister of ISED. Both have put in place mechanisms to help FPT regulators develop and implement standardization priorities.

At the policy and strategic level, there are three overarching advisory bodies:

- SCC's PTAC;
- the National Public Safety Advisory Committee (NPSAC), also supported by SCC; and
- the Canadian Table for Harmonized Construction Codes Policy, supported by the NRC (this newly created body supersedes the Provincial/Territorial Policy Advisory Committee on Building Codes).

PTAC

PTAC is a statutory committee of SCC. It is composed of members appointed by the governments of all provinces and territories. The main objectives of the committee are to provide advice to SCC on P/T standardization priorities, advise and make recommendations to the council on matters related to voluntary standardization, and to promote cooperation and communication. Important focus areas have been regulatory reform and the alignment of mandatory standards and safety codes between provinces and territories.

NPSAC

NPSAC is composed of senior officials from provinces and territories responsible for electrical, plumbing, elevators, amusement devices, oil, gas, propane, boilers/pressure vessels and nuclear safety. It was created in the early 1990s through a memorandum of understanding (MOU) between jurisdictions. Although members do vote on resolutions, it is not a decision-making body. Each participating jurisdiction is called upon to follow through on resolutions through their respective accountability chains. NPSAC enables senior decision makers to exchange information and set policy objectives for public safety including harmonization of codes and standards across jurisdictions. Members present jurisdictional updates including plans for new regulations. They also discuss emerging issues with the view to take national approaches when possible.

Many NPSAC members are looking at risk-based approaches to enforcement and inspections in order to apply scarce resources to higher-risk areas. They are also looking at adopting standards emanating from other regions of the world when new technologies are deployed in the Canadian marketplace and incorporating them in existing safety codes. For example, industrial bio-digesters manufactured in Europe have been installed in Canada and licensed for operation based on European standards adopted in provincial regulation. In exceptional cases, NPSAC can collectively fund the development of new standards.

As a policy-setting body, NPSAC provides support and guidance to various RAABs regarding horizontal issues such as the implementation of trade agreements, regulatory reconciliation

and the emergence of uncertified products in the Canadian marketplace through e-commerce.

Canadian Table for Harmonized Construction Codes Policy

As indicated above, the NRC has been coordinating the construction codes development system since the 1930s. With core funding provided by the federal government in 2022, construction codes are now available free of charge to all stakeholders and users. A new governance model has been set up to streamline the development and timely adoption of these codes by all jurisdictions. Deputy ministers accountable for building regulations provide policy oversight through the table. As Figure 3 shows, the governance model established a Canadian Table for Harmonized Construction Codes Policy.

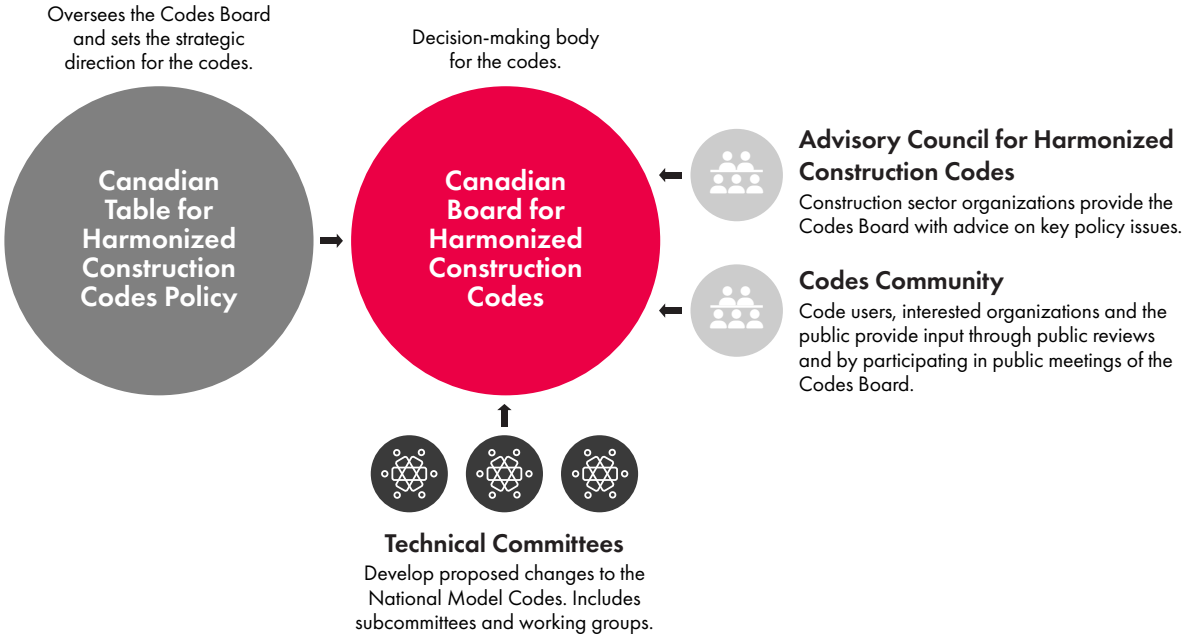
RAABs

As indicated above, provinces and territories have exclusive jurisdiction over a wide range of sectors such as electrical, buildings and infrastructure, fire, plumbing, oil, gas, propane, boilers and pressure vessels as well as elevators and amusement rides. They have developed a unique approach to manage health, safety and security issues by creating various positions of chief inspectors.

Generally reporting directly to ministers, chief inspectors are mandated to enforce safety regulations. By virtue of their authority to enforce health and safety regulations, chief inspectors wield considerable influence over Canada's standards and safety codes system. They are expected to propose the adoption of standards, safety codes and regulations to ministers for approval. Starting in the 1930s, chief inspectors began to create national advisory bodies to exchange information and set standardization priorities. These bodies liaised with industry, experts and relevant SDOs to set the right standards. They also engaged with certification bodies to oversee certification programs. Over time, a series of advisory councils made up of regulators and industry were set up. Regulators created committees and organized in camera sessions to exchange information, set standardization priorities and provide guidance to SDOs and industry.

Since 2016, SCC began to refer to advisory committees composed of chief inspectors and regulators as RAABs. These regulators have been formally recognized as AHJs over standards,

Figure 3: Governance Model to Harmonize Construction Codes in Canada



Source: https://nrc.canada.ca/en/diagram-new-governance-model-harmonize-construction-codes-canada.

technical specifications, safety codes and related conformity assessment programs. MOUs have been signed between SCC and some AHJs to clarify roles, responsibilities and accountabilities. RAABs accountable for maintaining and adopting specific safety codes are presented below. One should note the wide variety of mechanisms used by regulators to set standardization priorities and engage with stakeholders.

Canadian Advisory Council on Electrical Safety

The Canadian Advisory Council on Electrical Safety (CACES) was created by the CSA to provide guidance and support for its electrical standards and conformity assessment business lines. The CSA has been publishing the CEC (CSA C22.1) since 1927 and manages more than 700 electrical standards and application tools. The CEC provides requirements for the safe installation and maintenance of electrical equipment in Canada, and CSA electrical standards address items such as circuit breakers, wiring and electrical products as well as more sophisticated equipment for electrical controls and laboratory use.

CACES is composed of members from industry, consumers and regulators. Chief inspectors accountable for electrical safety meet and make decisions via a regulators committee under CACES. Chief inspectors hold in camera sessions where they discuss technical issues associated with the CEC, the need for new electrical standards, defective and counterfeit products, and conformity assessment. They are also accountable for the maintenance and approval of technical specifications. The regulatory committee of CACES is the AHJ for the CEC electrical safety standards/technical specifications.

Like other safety codes, the CEC is referenced in jurisdictions across Canada. Most provinces and territories adopt the CEC through a static reference, sometimes with a schedule of amendments added to the code to address "local conditions" and a unique designation for the code (for example, the Ontario Electrical Safety Code).

Association of Chief Boiler and Pressure Vessel Inspectors

The Association of Chief Boiler and Pressure Vessel Inspectors (ACI) was created in the early 1960s. It is composed of FPT regulators, chief inspectors, and representatives from the National Energy Board, the Canadian Nuclear Safety Commission and the National Board of Boiler and Pressure Vessel Inspectors. The span of accountability includes all fuels, gas, propane (including liquefied natural gas and compressed natural gas), hydrogen, boilers and pressure vessels. Safety codes managed by ACI include the CAN/CSA B149 Gas Code; the CSA B51 – Boiler, Pressure Vessel, and Pressure Piping Code as well as related standards and technical specifications. Chief inspectors are accountable for the installation of natural gas appliances, equipment, components and accessories where gas is to be used for fuel purposes, and propane storage/handling as well as the management of permits, licences and registration numbers for boilers and pressure vessels.

ACI provides a forum for regulators to exchange information regarding accidents and incidents involving pressure equipment and methods to prevent recurrence; new developments, installations and new regulations; uniform standards for power engineers and plant operators; and boiler and pressure vessel inspectors, welders and non-destructive examiners. Regarding standards and safety codes, ACI sets priorities for the development, revision and research of safety codes and standards. It aims for uniformity and harmonization in the application and enforcement of standards. It is the AHJ for the sector. Chief inspectors liaise with gas industry representatives through the Interprovincial Gas Advisory Council.

Canadian Advisory Council on Plumbing

The Canadian Advisory Council on Plumbing (CACP) is a joint committee of industry, regulators and relevant accredited conformity assessment organizations focusing on plumbing safety codes, standards and technical specifications. It looks at the Canadian Plumbing Code, the more than 100 standards incorporated by reference in the safety code and additional standards referenced in P/T regulations.

The CACP acts in an advisory capacity to participating accredited organizations on matters pertaining to standards and conformity assessment programs affecting plumbing. It provides a forum for industry, regulators and product certification organizations to share new concepts and ideas; to discuss policy and programs; and to review innovations and new technologies that affect plumbing standards,

and the certification and testing of plumbing products. The regulators responsible for plumbing regulations meet through a regulatory committee.

Council of Canadian Fire Marshals and Fire Commissioners

The Council of Canadian Fire Marshals and Fire Commissioners assists fire marshals, fire commissioners and regulators in managing emergency safety-related safety codes such as the Fire Code and relevant standards. The council also aims to apply a cohesive and consistent national approach to fire service issues and concerns. It does not have formal standing as a RAAB with SCC.

Chief Inspectors for Elevating Devices

Chief inspectors for elevating devices are not formally engaged in a RAAB. Instead, they coordinate standards development activities through a joint Canada-US Technical Committee on Elevator and Escalator Electrical Equipment managed by the CSA and its US counterpart, ASME. This committee oversees a number of cascading standards and safety codes under the jurisdiction of the chief inspectors.

CBHCC

FPT building and fire safety officers are members of the CBHCC, which is the decision-making body for the construction codes.[8] Secretariat services are provided by the NRC. The board is supported in its work by standing committees that report to the board. The standing committees are responsible for various technical areas in the construction codes. Standing committees, in turn, rely on short-term task groups, working groups and advisory groups to study specific issues and make recommendations. Members of these committees and groups are drawn from all segments of the construction industry: regulators, fire services, architects and engineers, manufacturers and product suppliers, building owners and developers, and building users. They are appointed as individuals, not as delegates from a specific association or company, and are selected in a way that provides representation from all geographic regions of the country.

8 See https://nrc.canada.ca/en/certifications-evaluations-standards/codes-canada/how-nrc-supports-codes-development-system.

Implications for a Future Privacy RAAB

With the information presented above, one can make the following observations about a future privacy RAAB. First, it is clear that precedents do exist whereby FPT regulators get organized through advisory committees or councils focused on setting standardization priorities. Many possible avenues can be explored, ranging from a formal table pursuant to a binding agreement referenced in the CFTA, a multi-stakeholder advisory council or a regulatory committee, to an informal subcommittee of regulators as part of a larger technical committee overseeing a specific standard or safety code.

There are ample precedents confirming that chief inspectors and other regulators have delegated authority not only to meet and exchange information on emerging issues but also to provide advice to stakeholders on voluntary standardization. Regulators also have the delegated authority to participate in voluntary standardization activities and to vote on the adequacy of voluntary standards leading to the publication of NSCs.

It is also clear that chief inspectors and regulators have focused their attention on the development and maintenance of safety codes (or model codes) as the preferred compliance mechanism. Safety codes themselves set a series of requirements regarding the "what" to do, the objectives to aim for and the principles to apply in order to comply with a given regulation. Safety codes are always accompanied by annexes containing individual standards that specify requirements for specific products and components as well as the testing methods to demonstrate compliance with the standards.

Third, although jurisdictions intend to adopt new versions of safety codes as is when they are published, there is ample scope for them to introduce amendments to a code or to skip adoption altogether if necessary.

Finally, RAABs operate without restriction as to which specific SDO or policy body to engage with and for how long. Regulators operate in a free market environment. A future privacy RAAB will be able to choose to engage with a small

grouping of SDOs, presumably only those that can support the development of standards and technical specifications to "bake in" privacy in relevant products and devices, and support the development of standards supporting compliance with privacy legislation at the organizational level.

Standards in FPT Regulations

Although practices vary from one jurisdiction to the next, developed countries tend to reference a large number of standards and conformity assessment obligations in regulations. The practice is defined as incorporation by reference. This section provides an overview of standards incorporated by reference in FPT regulations. The information is generated by SCC through its Monitoring Standards in Regulations initiative.

Standards in Federal Regulations

At the federal level, there were 1,535 standards referenced at the federal level in 2020 (SCC 2021). Communications made by SCC before the pandemic showed 1,377 references to standards in 135 Canadian federal regulations maintained by 19 departments and agencies. Examples of regulations include those covering occupational health and safety, construction and infrastructure energy efficiency requirements, environmental protection, consumer products, electrical, oil and gas, elevators, pressure vessels, medical devices and organic foods. Figure 4 presents a distribution of references to domestic, other national or regional SDOs, or international standards in federal regulations and related instruments in 2018.

Standards in Provincial Regulations

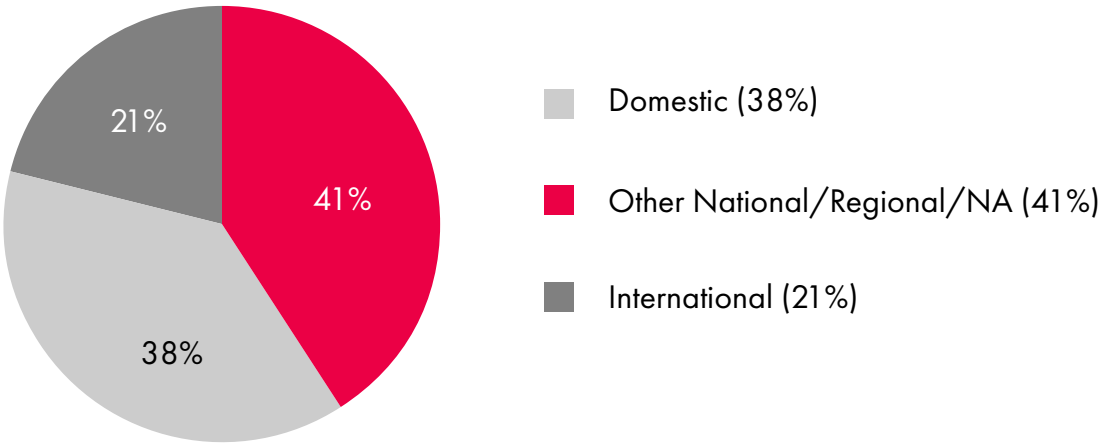
At the P/T level, there were 4,538 standards referenced at the federal level in 2020 (ibid.). SCC's annual report for 2018–2019 shows 4,461 references to standards in P/T regulations as shown in Figure 5.

Incorporation Methods

Using standards as a complement to regulations can provide many benefits to regulators, industry and consumers alike.

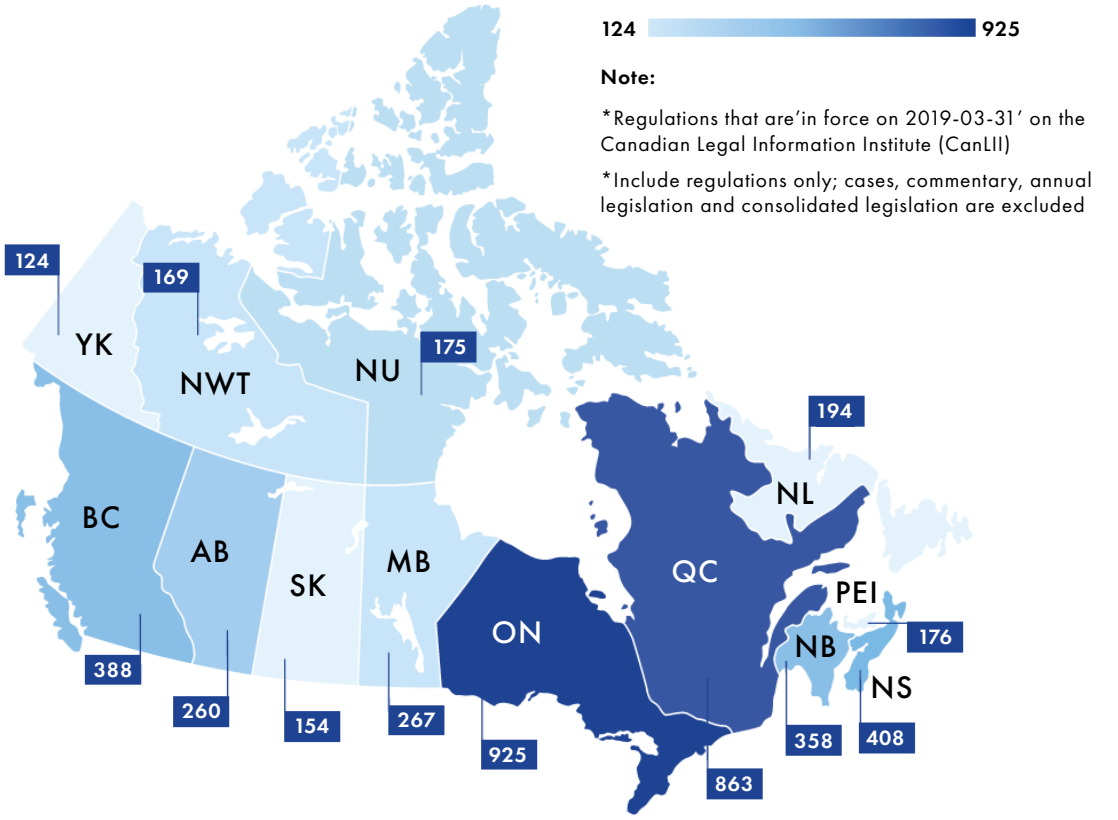
For regulators, there is no need to "reinvent the wheel" when addressing common issues. If we take electrical safety and interoperability, for example, regulators benefit from participating, along with industry and consumers, in the development and maintenance of a common electrical code that can be adopted by all jurisdictions when

Figure 4: Distribution of References to Standards in Federal Regulations



Source: Girard (2018).

Figure 5: Distribution of Standards in P/T Regulations



Source: SCC (2019c, 37).

a new edition is published. Adopting common standards also meets WTO obligations to reduce non-technical barriers to trade.

For industry, the adoption of common standards by regulators reduces the need for multiple testing and certification to access P/T markets. For consumers, the adoption of common standards makes it easier to acquire products that can operate in multiple environments and that are certified to perform to a given benchmark with the added advantages of increased competition and lower prices. One of the most critical consumer aspects is trust: standards provide consumers with a basis for trust. Labels and certification marks provide consumers with something they can trust and an organization that is accountable for safety, reliability or efficiency claims.

There are many possible ways to reference standards and technical specifications to support regulatory objectives.

Directly into a Statute or Regulation

Although rare, a regulatory authority may choose to reproduce the wording of a standard and/or accreditation program directly into the legislative/regulatory text. As mentioned in the introduction, a good example of this method of incorporation is the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000 where the CSA's Model Code for the Protection of Personal Information was reproduced in a schedule. Regulators also sometimes incorporate a specific paragraph or sentence from a given standard in regulations. It should be noted that references to specific clauses or subclauses, tables, figures or annexes of a standard should always be dated. This is because any amendment to, or revision of, a standard could lead to an alteration of its internal numbering (ISO/IEC 2014).

Static References

Regulators often use the static method of incorporation, also called direct dated references. Direct dated referencing is when the number and title of the standard are referenced and used with its date of publication (see Box 1). This means that only a particular edition of a standard can be used. This can help provide legal certainty by indicating the exact technical solution that may be used to comply with the regulation. Such legal certainty can help give assurance to the regulator and clarity for those who must comply with the law. This is the most restrictive reference.

Box 1: Static Reference Example

The AI system shall conform with CAN/CIOSC 101:2019: Ethical Design and Use of Automated Decisions Systems.

Source: Author.

As Amended from Time to Time

Regulators also use the "as amended from time to time" incorporation method, also called direct, undated references. A regulation would quote only the number and title of a specific standard and not the date (see Box 2). In the case of a revision of a referenced standard, the regulation itself does not need to be adapted as the reference automatically corresponds to the latest edition of the standard. In other words, the regulation allows the use of subsequent revised editions of the same standard. This allows for the regulation to reflect new technologies, processes or approaches without amending it.

Box 2: As Amended from Time to Time Example

The AI system shall conform to the latest edition of CAN/CIOSC 101: Ethical Design and Use of Automated Decisions Systems.

Source: Author.

Referencing a Standard with Additional Requirements

Regulators sometimes determine that adherence to a given standard is not enough in itself to meet legislative objectives and will spell out additional requirements in the regulation. A "weak" voluntary technical standard can therefore be incorporated in a regulation with additional requirements spelled out. For example, there are many standards covering the energy efficiency performance of consumer goods and appliances. However, some jurisdictions will set the energy efficiency bar higher and spell out amendments to the standards in the regulatory text. When the new regulation is published, it may get noticed by technical committees in charge of the standard and may result in updates to subsequent editions to keep the document relevant.

Lists of Recognized Standards

Regulators may be faced with ongoing and significant changes in technologies and processes that are subject to regulations. One approach would be to update a regulation on an ongoing basis to make the necessary additions and subtractions of relevant standards as required. However, this process can be costly and time consuming for the regulatory authority.

A more flexible approach is to maintain an official list of recognized standards on a government department website. For example, Health Canada maintains the Therapeutic Products Directorate List of Recognized Standards for Medical Devices. It is published by authority of the minister. The list, which contains more than 200 standards pertaining to medical devices, is regularly updated without the need to update the medical devices regulations. New standards are added, new editions of existing standards replace older versions and standards associated with discontinued products or processes are removed. The list is maintained "to provide guidance for manufacturers on the use of standards in demonstrating compliance with the *Safety and Effectiveness Requirements* (section 10 to 20) and *Labelling Requirements* (section 21 - 23) of the *Canadian Medical Devices Regulations* (Regulations)." Guidance documents are used as

administrative instruments. They do not have force of law but allow for flexibility in approach.[9]

This approach, used by federal departments to support other regulations such as the transportation of dangerous goods,[10] is not unique to Canada. Following Brexit in 2020, the UK government introduced a master "List of Designated Standards" available on a government website. Businesses can use the list to demonstrate that their products, services or processes comply with essential requirements of legislation.[11] The UK government created a designation process that allows the British Standards Institution (SCC's equivalent in the United Kingdom) to submit new standards for consideration by government officials. Australia also maintains evergreen lists of mandatory/recognized standards on government websites covering issues such as high-risk consumer products[12] or medical devices.[13]

Procurement

In some cases, it may be adequate to merely encourage the use of standards on the assumption that their voluntary take-up by the market means that regulators' objectives are being met (for example, by enhancing the quality of products or services in a particular sector). Such measures do not require the creation of legal instruments but can be achieved through government policy in targeted areas such as procurement. In cases where this occurs, the standard may become the de facto tool for market access. For example, in March 2019, the Canada Mortgage and Housing Corporation issued a "Request for Proposal for Unstructured Data Archiving Solutions." The document requires that a bidder comply with the ISO 27001:2013 standard to establish, implement, maintain and continually improve its information security management system (ISMS) (Canada Mortgage and Housing Corporation 2019).

Digital Governance Standards and Regulations

The use of standards and certification programs to support compliance with regulatory objectives is not limited to traditional, established sectors. Authorities involved in the development of digital governance regulations are also planning to use standards and third-party certification as compliance mechanisms. It is still early days, but we can see that standards will play an important role in both tangible products and intangibles. In Canada, Ontario's draft AI commitments and actions recognize the importance of referring to standards when developing AI rules and requirements. And following consultation with Ontario's public, the province heard the third-most important action for AI to serve all Ontarians, according to respondents, was to "engage with sector leaders and civil society to develop a standard for 'trustworthy AI' and a process to certify that vendors are meeting the government's standard."[14]

Additionally, one CIOSC notes the government reference and use of CIOSC's NSC on automated AI decision systems in the recent release of its beta principles for the use of ethical AI. This includes guidance for the Ontario Public Service to document how the use of data-driven technologies in the process, program or service aligns with ethical principles, governance frameworks and industry standards.[15]

Internationally, the EU Artificial Intelligence Act tabled in 2021 states that standards and certification will be used as the preferred compliance mechanism to frame high-risk AI applications in the delivery of products, devices, systems, networks and services. The European Union will require the adoption of enterprise-wide quality management and risk management standards for organizations developing algorithms as well as for organizations using them. Organizational compliance with these management system standards will be audited

9 See www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/standards/list-recognized-standards-medical-devices-guidance.html.

10 See https://tc.canada.ca/en/dangerous-goods/list-safety-standards-csa-cgsb-transport-canada-standards.

11 See www.gov.uk/guidance/designated-standards.

12 See www.productsafety.gov.au/product-safety-laws/safety-standards-bans/mandatory-standards.

13 See www.tga.gov.au/standards-guidelines-publications-medical-devices-ivds.

14 See www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework-consultations#section-3.

15 See www.ontario.ca/page/beta-principles-ethical-use-ai-and-data-enhanced-technologies-ontario.

by independent third parties. New certification schemes are expected to be developed to cover AI systems to be deployed in the services sector.

Additionally, the European Union has labelled AI applications embedded in standardized consumer products and machines as high-risk AI. New performance standards will be developed to frame the use of AI chips in various product categories. New testing protocols will be developed to certify that products and devices using AI chips are safe and trustworthy (European Commission 2021).

The UK government has already signalled its intention to implement a high-risk AI regime that will be deemed equivalent to the EU AI Act (UK 2021). As such, it will regulate high-risk AI using standards and certification programs in regulation. In December 2021, it signalled its intention to become a world leader in the development of a series of supportive standards and certification programs through the creation of an AI Standards Hub.[16] The ultimate objective of the hub is to create an effective AI assurance ecosystem through the management of appropriate levels of assurance based on risk across sectors and domains. As a public/academic/private collaborative, it may be a model of interest to Canadian privacy regulators.

In the United States, the National Institute of Standards and Technology released its long-anticipated Artificial Intelligence Risk Management Framework (AI RMF 1.0) standard in January 2023. The framework was developed following an executive order from the White House in 2020. It provides voluntary guidance for organizations to use when managing AI risks to individuals, organizations and society by incorporating trustworthiness considerations into the design, development, use and evaluation of AI products, services and systems. It is anticipated that this new standard will be applied by all federal government agencies using high-risk AI and be mandated within organizations doing business with the government. This standard is also expected to be adopted by states and other national governments (National Institute of Standards and Technology 2023).

16 See https://aistandardshub.org/; for background information, see www.gov.uk/government/news/new-uk-initiative-to-shape-global-standards-for-artificial-intelligence.

Privacy Standards and Compliance Mechanisms

As mentioned in the introduction, Canadian privacy regulators led the way in the development of voluntary privacy standards. In the 1990s, Ontario's privacy commissioner and two officers from the Ontario and Canadian privacy commissioner's office became members of the CSA Technical Committee on Privacy (reporting to the Steering Committee on Business Management Systems). The committee drafted the CSA Model Code for the Protection of Personal Information. The model code was published as an NSC in March 1996. It proposed 10 principles to organizations on collecting, using, disclosing and protecting personal information. It also outlined in broad terms the rights of individuals to access personal information about themselves and, if necessary, to have the information corrected (CSA 1996).

When published, the CSA model code was seen as the cornerstone of a new voluntary privacy compliance framework. Soon after the code was published, CSA Group introduced a workbook to assist organizations in applying the code and guidance documents to implement privacy codes of practice. Compliance with the code required the installation of systems and procedures to track compliance with the 10 principles. Although implementing the code could be a time-consuming task, experts argued that once in place, "the ongoing maintenance of systems and procedures to meet the Standard should become a routine operation" (CSA Group 2004).

To enable compliance reporting, the Quality Management Institute, a subsidiary of CSA Group, offered three levels (or tiers) of recognition:

- Tier 1: declaration of the organization's intent to apply the CSA code;
- Tier 2: verification that the CSA code has been implemented to an acceptable standard; and
- Tier 3: registration (CSA Group 2004).

At the time, no other country had attempted to develop and implement a voluntary compliance framework for privacy protection. It raised a number of intricate questions that had never been addressed before. As the years went by, pressure

built up to make the model code mandatory. In 2001, the CSA Model Code was copied directly into a schedule in PIPEDA. However, the accompanying workbook, guidance documents and codes of practice developed by the CSA were not referenced in regulations or guidance documents.

As jurisdictions began to introduce privacy legislation in Canada and around the world, SDOs and consortia began to publish voluntary standards and guidance documents to assist organizations in their compliance efforts.

The first wave of standards focused on ISMS such as the ISO 27000 series. The ISMS family of more than 30 standards provides detailed guidance on privacy, confidentiality and IT/technical/cybersecurity issues.[17]

A second wave of ISO/IEC standards was aimed at privacy information management systems for organizations. In 2019, ISO published the first international standards for privacy information management. ISO/IEC 27701 specifies requirements "for establishing, implementing, maintaining and continually improving a privacy-specific information security management system"; in other words, a privacy information management system for protecting personal data.[18]

A third wave focused on products and services. In January 2023, ISO published ISO 31700-1:2023 Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements (ISO 2023). This document establishes high-level requirements for privacy by design to protect privacy throughout the lifecycle of a consumer product, including data processed by the consumer (ibid.).

A new bar was set with the entry into force of the GDPR, which came into effect in 2018 to harmonize data protection laws across the European Union. Enforced by the data protection authorities in each EU member state, the GDPR applies to any organization that processes or holds the personal data of data subjects residing in the European Union.

On the one hand, the regulation is quite specific regarding mandatory documents and forms that organizations must create and use, from the Personal Data Protection Policy to data-processing agreements. On the other hand, the GDPR does not yet reference mandatory standards to facilitate compliance. And there are no official lists of recognized standards either.[19]

Nevertheless, voluntary international standards have been identified by experts to assist organizations in meeting specific requirements. For example, in 2018, SCC invited the Canadian Advisory Committee on the General Data Protection Regulation (CAC-GDPR) to propose a list of ISO/IEC standards that would facilitate compliance with the regulation. The experts submitted a list outlining approximately 20 ISO/IEC standards. Table 1 presents key ISO/IEC voluntary standards that have been identified by the CAC-GDPR to facilitate compliance with the regulation. They noted, however, that the regulation is complex and that complying with standards alone will not be sufficient to comply with the GDPR (SCC 2020).

Uncertainty about what standards to use is bound to grow: the ISO/IEC list is only the tip of the iceberg in the universe of standards, technical specifications and codes of practice that organizations can use to demonstrate due diligence to privacy legislation. Following the entry into force of the GDPR, a growing number of standardization initiatives have been launched regarding personal data privacy, portability and consent. In Europe, the Internet Privacy Engineering Network is looking at standards development for data privacy.[20] In Canada, the Global Privacy and Security by Design collective offers a Privacy by Design certification program based on the Privacy by Design seven principles.[21]

Examples of standards consortia focusing on sectoral applications with an impact on privacy include the Clinical Data Interchange Standards Consortium, which deals with health-care related medical research data, to enable information system interoperability and to improve medical research and related areas of health care.[22]

17 See https://en.wikipedia.org/wiki/ISO/IEC_27000-series; www.iso.org/standard/73906.html.

18 See www.iso.org/standard/71670.html.

19 See https://gdpr.eu.

20 See https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en.

21 See https://gpsbydesign.org/get-certified/.

22 See www.cdisc.org/standards.

Table 1: ISO/IEC Standards Facilitating Compliance with the GDPR

No.	Title	Context
ISO/IEC 15944-5:2008	Information technology — Business operational view — Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints	Facilitates the creation of an electronic business architecture reflecting external requirements and restrictions such as jurisdictional domain. Will help organizations adopt the GDPR in their practices.
ISO/IEC 15944-12:2020	Information technology — Business operational view — Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)	Provides a framework to identify external requirements and restrictions related to personal data for recorded information in business transactions.
ISO/IEC 19944-1:2020	Cloud computing — Cloud services and devices: data flow, data categories and data use — Part 1: Fundamentals	Creates a foundation for categorizing data that crosses between customers and cloud providers. Includes categories such as health data where the GDPR is applicable.
ISO/IEC 19944-2:2022	Cloud computing and distributed platforms — Data flow, data categories and data use — Part 2: Guidance on application and extensibility	Provides guidance on how to apply 19944-1 and includes privacy-related examples.
ISO/IEC 20546: 2019	Information technology — Big data — Overview and vocabulary	Establishes clear terms and definitions to facilitate the understanding of concepts around big data.
ISO/IEC 20889: 2018	Privacy enhancing data de-identification terminology and classification of techniques	Elaborates on the use of de-identification. In line with privacy principles found in ISO/IEC 29100, its use can enhance the protection of personal data.
ISO/IEC 22624: 2020	Information technology — Cloud computing — Taxonomy based data handling for cloud services	Incorporates further data classification and geolocation information. Highlights where the GDPR needs to be considered.
ISO/IEC 22678: 2019	Information technology — Cloud computing — Guidance for policy development	Highlights that existing policies may need to be changed and interpretations around the GDPR might be required to demonstrate due diligence.
ISO/IEC 23751: 2022	Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA)	Explores how data-sharing agreements can be established. This permitted sharing concept can impact how the GDPR is applied.
ISO/IEC 27001: 2013	Information technology — Security techniques — Information security management systems — Requirements	Provides a framework for the creation of an information security management system to help prevent data breaches and facilitate GDPR compliance.
ISO/IEC 27002: 2013	Information technology — Security techniques — Code of practice for information security controls	Provides guidance on how to apply 27001. Helps in selecting the right controls for the establishment of an ISMS.

Table 1: ISO/IEC Standards Facilitating Compliance with the GDPR (continued)

No.	Title	Context
ISO/IEC 27018: 2019	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	Establishes a framework to protect PII in public cloud computing. This enhanced protection for PII can help improve the protection of personal data, an essential element of the GDPR.
ISO/IEC 27701: 2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	Addition to ISO/IEC27001 and ISO/IEC27002. Provides additional guidance to maintain a privacy information management system.
ISO/IEC 29100: 2011	Information technology — Security techniques — Privacy framework	Provides a PII security framework for ICT to improve the handling of personal data. Offers additional support for the GDPR compliance process.
ISO/IEC 29151: 2017	Information technology — Security techniques — Code of practice for personally identifiable information protection	Highlights guidance for the application of controls to limit exposure to data breaches, a key objective of the GDPR.
ISO/IEC 29184: 2020	Information technology — Online privacy notices and consent	Provides a foundation for informed customer consent of data usage and closely aligns with GDPR requirements.
ISO 31700: 2023	Consumer protection — Privacy by design for consumer goods and services	Provides a road map for organizations to design and implement privacy features and controls into their products. It addresses privacy issues raised by the GDPR.
ISO/IEC 38500: 2015	Information technology — Governance of IT for the organization	Provides a governance model to establish an efficient IT infrastructure, which can facilitate the transition toward a GDPR-compliant model.
ISO/IEC 38505-1:2017	Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data	Provides guidance for organizations on how to apply ISO/IEC 38500.

Source: SCC (2020b)

SAE International is creating a consortium to develop best practices and standards for storing and sharing data acquired from shared micro-mobility services.[23] Global initiatives include Solid, which aims at decoupling data from applications by offering a new architecture for the Web. Led by Tim Berners Lee, inventor of the World Wide Web, the initiative would allow individuals to choose where their data can be used and for what purpose by creating individual "Solid Pods."[24]

Global platforms have also put pen to paper. The Data Transfer Project led by Google, Facebook, Microsoft and X (formerly known as Twitter) started in 2018 and aims at developing technical standards for personal data portability "so that all individuals across the web could easily move their data between online service providers whenever they want" (Jennings 2018). Once these standards are in place, they could also be used to manage direct and automated data transfers between a source and a data access point (Data Transfer Project 2018).

23 See www.sae.org/micromobility/.

24 See https://solidproject.org.

This overview represents only a cross-section of initiatives aimed at standardizing the privacy space. Somehow, regulators will have to navigate this landscape, assess the merits of competing programs and provide appropriate guidance to organizations aiming to comply with privacy legislation nationally and internationally.

Conclusion: Toward a Privacy RAAB

As outlined in this paper, there is a strong rationale for the creation of a privacy RAAB in Canada. Although privacy legislation can apply to any organization in Canada, regulators are not currently organized to guide the development and implementation of broad-based standards, codes of practice and compliance programs. Through the creation of a privacy RAAB, both FPT privacy commissioners and regulators can coalesce and directly engage with standardization bodies without jeopardizing their neutrality and independence, nor limiting their ability to perform enforcement activities. It borrows from approaches that have been set up by FPT regulators accountable for the health, safety and security of consumer products, devices, processes and infrastructure.

It makes sense for privacy regulators to engage with Canadian organizations as a whole rather than through the provision of advice to individual firms. Under the status quo scenario, organizations can be challenged to understand what is required of them, leading them to either forego innovation to minimize risk, or to innovate in a manner that does not respect privacy rights. Through open and transparent standardization fora and processes, from advisory bodies to technical committees and working groups, privacy regulators can help set consensus-based standards.

In addition, the governance framework that has been established around international and national standards development sets a bar to ensure broad-based participation from all stakeholder groups and transparency as well as predictability in how documents are developed, approved and maintained. It is true that many innovative approaches have been tested by consortia and open-source platforms to develop digital governance rules. However, governments and industry continue to rely on the formalized standards development process adhering to WTO fundamental principles. This approach may be slower and somewhat plodding, but it is seen as trustworthy.

Strong precedents have been set by chief inspectors to undertake the following activities:

- → Engage with stakeholders and SDOs on the standardization needs of regulators.
- → Identify gaps in standardization and propose approaches to SDOs to fill these gaps.
- → Set standardization priorities with other regulators.
- → Review national and international standards, technical specifications and codes and determine whether they are suitable for adoption in their respective jurisdictions.
- → Participate in standards development activities when appropriate, notably for new national standards that are intended to become mandatory.
- → Select the right accreditation framework and approach for the development and approval of codes of practice.
- → Engage with industry associations and professional classes regarding the development of standardized compliance programs and codes of practice.
- → As the AHJ for standards, technical specifications, compliance programs and codes of practice, engage with SCC regarding the creation of supportive accreditation programs and the negotiation of mutual recognition agreements.
- → Generally, aim to promote regulatory reconciliation and minimize divergences in regulatory approaches when possible but ultimately recognize that each jurisdiction maintains full authority to adopt, adapt or reference any standard and/or compliance program, or refrain from doing so.

There is also ample precedent confirming that chief inspectors, as other regulators, have delegated authority to undertake these activities, not only to meet and exchange information on

emerging issues but also to provide advice to stakeholders on voluntary standardization.

In addition, regulators have the delegated authority to participate in voluntary standardization activities and to vote on the adequacy of NSCs because it does not bind them to adopt these documents in their respective jurisdictions.

As this paper has shown, many avenues can be explored to create the right advisory body for privacy regulators. It can take the form of a multi-stakeholder advisory council where regulators meet during in camera sessions and formally engage with other members representing industry, consumers, software developers and SDOs in a dialogue on standardization priorities through open fora. It can also take the form of a regulatory committee composed exclusively of privacy regulators. Through that mechanism, it can limit its interactions to relevant SDOs, SCC and professional associations and, in turn, mandate these bodies to connect with relevant stakeholders and develop the right standards and compliance programs. Ultimately, the choice of governance mechanism really depends on the short- and long-term priorities of Canada's privacy regulators as a community.

However, to get to the stage where a privacy RAAB becomes operational, two challenges must be overcome. First, it should be acknowledged that standardization in Canada is not a top-of-mind issue for most decision makers, consumers or regulators, including privacy regulators. Although tens of thousands of Canadians routinely participate in standards development activities nationally and internationally, these activities take place under the radar. General awareness about the features and outputs of Canada's standardization system is generally low among consumers and senior decision makers. The challenge for privacy regulators will therefore be to learn about the features and rules of the standardization system internationally and nationally.

Secondly, the Canadian system is not straightforward; it has been described as complex, even opaque by some. For example, with a few exceptions such as the CBHCC, the connections between Canadian regulators and stakeholders engaged in standardization are almost invisible to the uninitiated. Most of the regulatory advisory councils and policy committees focusing on standards and model codes described above operate through loosely worded administrative agreements and low-cost secretariats. Although their recommendations and guidance can be consequential for Canadians, one would be challenged to learn about any of these bodies by performing searches on regulators' websites. The second challenge will therefore be to acknowledge the complexity of the Canadian standardization system, but question it when necessary, so that a new privacy RAAB can operate in an open and transparent manner to the benefit of all.

Annex: What Are Standards?

Although not visible to the average consumer, standards and conformity assessment activities keep the economy running. Standards describe the importance of a process, product, service or system. They provide a level playing field for industry and help build trust between participants in supply chains. They cover everything from the size of the simplest screw thread to the most complex IT network. They serve as a "handshake" between various components of systems and allow for interoperability by assuring that everyone is following the same standard. Standards also play a pivotal role in protecting the health and safety of consumers in a wide number of sectors including food and consumer products, security, infrastructure and the workplace.

Standards are generally taken for granted by consumers and citizens. Their presence and use make our devices and products work better, for example, by ensuring that the connection between a smart phone and a Wi-Fi network happens. A lack of standards does get noticed by consumers, for example, when travellers must use adapters to charge electronics in a foreign country, or when clothing or shoe sizes vary from one brand to the next. The push for standardization can lead to government intervention when one market participant refuses to adopt a standard. One example that has been unfolding for the past decade involves European regulators and Apple regarding the use of a common charging standard for mobile devices in order to reduce waste from incompatible chargers and cables (Ray 2022). Their misuse can result in spectacular failures, for example, when a US$180 million spacecraft disintegrated because the wrong measurement standard was inputted into the orbital insertion software by a contractor (Harish 2022).

Standards cover a wide spectrum of subjects, from definitions, ontology classifications, metrics, measurement, manufacturing techniques and processes, to delivery systems and beyond. They set out requirements, specifications, guidelines or model characteristics that can be consistently applied to ensure that products, materials, processes, systems and services perform as intended — qualitatively, safely and efficiently. And many are drafted in a way that allows another party to test and certify that a product, process or system meets the requirements of a specific standard. Put simply, they make things work, save organizations money, help innovations spread, and facilitate efficient trade among provinces, countries, economic regions and the international community.

The ISO uses the following definition for technology standards: "A document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context....Standards [moreover] should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits."[25]

Evolution of the International Standardization System

Thousands of organizations around the world are developing and maintaining more than one million standards and specifications. Many were created at the beginning of the twentieth century to support the emergence of new industrial sectors such as telegraphs, railways, steel, oil, motor vehicles, electricity, plumbing, boilers and pressure vessels, elevators, buildings and appliances. Some SDOs specifically focus on health and safety issues stemming from industrialization such as fire protection or occupational health and safety. Often, national professional associations such as those representing mechanical and electrical engineers as well as subdisciplines such as gas, water, fire, pressure vessels and elevators, created their own SDOs to develop and maintain the standards they needed to operate safely.

Health, safety and security issues have always been top of mind for those participating in standards development activities during the industrial age. Clearly, the standardization of pressure vessels, boilers, steel bridges, railways, elevators, pipelines or elevating devices brought costs down and allowed for interoperability. But as importantly, standards were seen as an effective tool to manage risk, to reduce the number and severity of accidents, and to save lives. Engineers responsible for product design,

25 See www.iso.org/obp/ui/#iso:std:iso-iec:guide:59:ed-2:v1:en.

manufacturers, operators, workers and consumers all had a stake in standards development.

After the Second World War, new international SDOs such as ISO were created, and older ones such as IEC and the International Telecommunication Union (ITU) expanded their scope as trade liberalization discussions were gaining traction. Competing national standards covering the same products and processes were increasingly seen as non-tariff barriers to trade. Truly international standards were needed to support globalization and international supply chains. Some argue that the international standards development process is similar in some ways to international treaty making.

As new sectors emerged in the 1960s, additional SDOs and new standardization activities began to support increasingly complex sectors such as plastics and chemicals, business machines, telecommunications, computers and information processing, avionics, laboratory testing as well as services and management systems standards covering quality, risk or the environment.

Up until recently, most SDOs required between 18 and 36 months to develop a new standard. This is, in part, due to the rules governing standards development and to the culture of the organizations and their membership. The standards development, comment and approval process is highly structured, with a mandatory cross-section of stakeholder representation throughout, and codified in specific stages, with built-in timelines for clause-by-clause review, comments and written disposition, voting and balloting.

These structured steps allow stakeholder groups to review, debate, comment, vote or sometimes block and delay the publication of a contentious document. Before the 1980s, in-depth discussions on various national approaches and best practices in place in different regions of the world had to take place before decisions could be made on the features of a new international standard. Means of communication were slower and less reliable back then than they are today, forcing participants to meet in person for extended periods of time and to wait for documents to be physically mailed. However, these timelines were accepted because product life cycles were much longer than they are today.

There is also a human dimension to the traditional technical standards development process. Members generally preferred to meet in person in order to build trust, understand other parties' perspectives, discuss issues thoroughly and even review contentious text line by line as a group, which adds time to the development process.

Given that time is of the essence, Canadian SDOs are now able to develop national standards within a year. SDOs operating in the ICT and digital governance spaces have adopted different approaches to further accelerate the standards development process. These organizations use online collaborative tools and software allowing participants to work on documents and meet exclusively remotely. New standards can be developed in months and updated annually to reflect new technologies and processes.[26]

The development of the international standardization system was not centrally planned by any stretch. Most international and industry-specific SDOs began small and remain not-for-profit organizations, even those managing tens of thousands of participants, standards catalogues exceeding 10,000 documents, global sales strategies and hundreds of employees. Many have become complex organizations that need to generate a steady stream of revenues as they do not benefit from government appropriations. Generally, SDOs do not charge large fees for individual members to participate in the standards development process. Many SDOs offer subscription fees for members to access standards in specific categories. Some large international SDOs such as ISO and IEC require member participation through national member bodies representing individual countries and charge these bodies annual fees to participate. Adoption of international standards is done through voting and balloting of individual member bodies (one country equals one vote).

This explains why *voluntary* standards are not free. Once developed, they become copyrighted documents. Standards get published and sold to users. Buyers include all players in supply chains from raw materials producers and parts, components and systems providers, to assembled goods manufacturers, product-testing laboratories and conformity assessment bodies. Some SDOs such as the CSA or Underwriters Laboratories have

26 See https://dgc-cgn.org/standards/get-involved/.

subsidiaries that generate revenues by performing conformity assessment services including prototype product testing and certification. A portion of the profits generated from certification services can be reinvested in standards development activities.

The situation is different for *mandatory* standards. In the last decade, Canadian SDOs, like their international counterparts, have moved to make mandatory standards and safety codes (that is, those that are referenced in regulations) accessible to users. Some allow view-only access through their websites, while others such as the Digital Governance Standards Institute make all their standards and specifications freely available to download.

Once a standard is developed, it does not stay static; it navigates through a periodic maintenance cycle. Technical committees will review the standards under their purview to make minor amendments and incorporate new features. For mature product lines, SDOs require a mandatory review of a standard every five years. If a standard needs significant changes, a new edition of the document will be issued. If no changes are required following a five-year review, the standard is labelled as stable — there is no need to purchase a new copy of the document. At the other end of the spectrum, standards associated with rapidly evolving technologies, products or processes can be updated at any time, sometimes multiple times a year. SDOs and resellers generally keep lists of clients who purchased or downloaded a given standard and advise them of new editions when available.

Principles for Standards Development and Maintenance

Standards are developed according to formalized rules that stipulate the processes to be followed involving engineers and other technical experts, regulators, and consumer interest and general interest groups. While standards are not neutral, they should balance competing interests in order to offer a technical solution that is broadly accepted and shares the benefits of technological compatibility as widely as possible. International standards development bodies must follow the WTO's six principles for standards development and maintenance. These principles are abstracted below as they shed light on the philosophy behind technical standards development activities both in Canada and internationally. Although adherence to these principles is time consuming, this overview also explains why this somewhat plodding process has remained relevant and sought after to this day.

Transparency

All essential information regarding current work programs, as well as on proposals for standards, guides and recommendations under consideration and on the final results, should be made easily accessible to at least all interested parties in the territories of at least all WTO members. Procedures should be established so that adequate time and opportunities are provided for written comments.

Openness

Membership of an international standardizing body should be open on a non-discriminatory basis to relevant bodies of at least all WTO members. This would include openness, without discrimination, with respect to participation at the policy-development level and at every stage of standards development. In particular, developing country members, with an interest in a specific standardization activity, should be provided with meaningful opportunities to participate at all stages of standard development.

Impartiality and Consensus

All relevant bodies of WTO members should be provided with meaningful opportunities to contribute to the elaboration of an international standard so that the standard development process will not give privilege to, or favour the interests of, a particular supplier or suppliers, country or countries, or region or regions. Consensus procedures should be established that seek to consider the views of all parties concerned, and to reconcile any conflicting arguments.

Effectiveness and Relevance

In order to serve the interests of the WTO membership in facilitating international trade and preventing unnecessary trade barriers, international standards need to be relevant and effectively respond to regulatory and market needs, as well as scientific and technological developments in various countries. They should not distort the global market, have adverse effects on fair competition, or stifle innovation and technological development. In addition, they should not give preference to the characteristics or requirements of specific countries or regions when

different needs or interests exist in other countries or regions. Whenever possible, international standards should be performance-based rather than based on design or descriptive characteristics.

Coherence

In order to avoid the development of conflicting international standards, it is important that international standardizing bodies avoid duplication of, or overlap with, the work of other international standardizing bodies. In this respect, cooperation and coordination with other relevant international bodies is essential.

Development Dimension

Constraints on developing countries, in particular, to effectively participate in standards development, should be taken into consideration in the standards development process. Tangible ways of facilitating developing countries' participation in international standards development should be sought. The impartiality and openness of any international standardization process requires that developing countries are not excluded de facto from the process. With respect to improving participation by developing countries, it may be appropriate to use technical assistance, in line with article 11 of the TBT Agreement. Provisions for capacity building and technical assistance within international standardizing bodies are important in this context (Wijkström and McDaniels 2013, 10–11).

It will be important to keep these principles in mind as we examine ways to standardize compliance with privacy requirements. Ideally, supportive privacy standards, model codes and compliance programs should be developed through a system that is widely seen as legitimate, impartial, independent and credible. Members of a privacy RAAB would be called upon to review international standards for possible adoption as mandatory standards in Canadian regulation or recognition as an acceptable means to achieve compliance. Having confidence that international SDOs adhere to these six principles will generate trust and facilitate the domestic review and adoption process. As explained in the next section, these principles also apply to accredited SDOs in Canada.

Key Features of Standards Development

Regulators are confronted with difficult choices when making decisions about their participation in standards development activities. Key features of standards development argue in favour of early and active participation by privacy regulators in order to ensure that published documents meet regulatory objectives. Early engagement by all also increases the probability that only one standard will be adopted by all jurisdictions, thereby reducing barriers to trade.

Standards Are Not Neutral

Participating in standards development means negotiating with others and making choices. It is about balancing the competing interests of those around the table in order to offer a technical solution that is broadly accepted and shares the benefits of technological compatibility as widely as possible. Although everyone can comment on a draft document, technical committee members yield significant influence over outcomes. The positions of chair and conveners of technical committees and working groups, who hold the pen and lead discussions, are highly sought after.

Setting standards is not about aiming for average performance. Generally, the goal of leading participants in the standards development process is to set the bar higher than current offerings in the marketplace and to aim for higher performance levels. As a result, standards generally end up using, or being based upon, proprietary technologies. From industry's perspective, the "prize" for participating in the development of a standard may therefore be to be first to market using the new standard applied to their product, service or process-embedded intellectual property (IP) they own in the performance features of a given document through either essential or non-essential patents.

Regarding health, safety and security requirements, standards set the bar for mandatory requirements. This obviously includes any legislative or regulatory requirement in force in leading jurisdictions. New editions of health and safety standards generally have higher levels of safety than what was required in previous versions of the same document, providing a clear pathway to improvement. This process requires participants to apply risk-based and evidence-

based approaches to assess which proposed additional requirement is the most cost-effective and will result in the greatest harm reduction.

Looking forward to future privacy standards, whether they are aimed at achieving organizational compliance or embedding requirements in new products or devices, having privacy regulators at the table can only be beneficial to all. Ongoing dialogue with regulators is not only helpful in understanding what needs to be achieved but also essential to draft appropriate clauses delineating specific requirements and in designing testing methods and verification processes that will adequately demonstrate compliance with regulatory objectives.

Once the Standard Is Set, the Die Is Cast

Participants in the standards development process will say that members invest significant amounts of time before coming up with the first edition of a voluntary standard. Entire industrial sectors may need to retool in order to meet new requirements. Prototypes need to get tested and products certified before they can be sold. The same is true for management system standards that apply to entire organizations. Significant changes to a management system standard can result in the need for new policies, procedures, job aids, training, controls and systems. As a result, committee members are generally wary of starting from a blank sheet again when the review process kicks in. Latecomers in the process are at a considerable disadvantage to embed their ideas if those are not included in the first edition of a document.

A similar rationale applies to new standards that are expected to become mandatory. Stakeholders simply will not have the incentive to invest time in a new mandatory standard unless regulators are confirmed participants in the process from the get-go. This may explain why, even though privacy legislation has been in place for almost 30 years, few privacy compliance programs have been successfully implemented in Canada. The same rationale applies to any existing standard that should be modified in the future to incorporate appropriate privacy compliance requirements. Looking forward, a privacy RAAB could encourage organizations, sectoral associations and chartered professions to invest the necessary time and resources toward privacy standards because there is a higher likelihood that the final product will be deemed acceptable by jurisdictions.

Organizations Benefit in Many Ways

As choices are made over competing ideas, processes or approaches, a new standard will quickly bring about technological, product and system certainty. Introducing a mandatory standard for all to comply with will reduce the cost of compliance at the firm level. When it comes to suppliers of systems and privacy-compliant products, a published standard will also shift the mode of competition from "differentiation" to "price competition." According to Dan Breznitz of the University of Toronto and Michael Murphree of the University of South Carolina:

> In a pre-standardization era, competition among products is defined by differentiation. Companies compete to attract unique communities of non-committed users by offering the most attractive option — defined through the best quality of service, range of capabilities, design, robustness or other unique proprietary features.... Once standards are set, however, the nature of competition rapidly changes. Standardization defines the central capabilities of a given technology — capabilities shared by all products regardless of company or country of origin. Where the capabilities are identical, the ability of providers to differentiate the standards-compatible products rapidly declines. Competition thus becomes defined by price as the standardized technologies are now commodities. (Breznitz and Murphree 2018, 8)

There is a plethora of proprietary consulting and software offerings for organizations aiming to achieve a reasonable level of compliance with privacy legislation and regulations. With the introduction of national voluntary privacy standards and compliance programs in the marketplace, one should expect price competition among firms providing software and services to organizations. This has the potential to expand compliance to a larger number of firms at a lower compliance cost overall.

Conformity Assessment

Once a standard is developed, it is important to ensure it is used as intended. Conformity assessment is a method to determine whether

products, services, processes, systems or persons meet specified requirements. Conformity assessment can involve certification, inspection and/or the testing of a product or system. It ensures that products and services meet required quality, safety and environmental standards, thus helping to safeguard the health and safety of consumers.

First-party conformity assessment refers to an activity that is performed by the person or organization that provides the object. In the European Union, for example, it is possible for a company to self-declare that their products are in conformity with EU rules by performing tests in-house and applying the relevant CE mark (the universally recognized mark affixed to products and components).

Second-party conformity assessment refers to a conformity assessment activity that is performed by a person or organization that has a user interest in the object. For example, a firm could ask one of its employees who is a member of a chartered profession to perform an assurance engagement and issue an opinion on compliance with a given standard. Although second-party conformity assessment is not used widely for certifying tangible products in Canada, this approach can be used by firms that aim to voluntarily declare conformance to a management system standard. This approach could be investigated by a future privacy RAAB.

Third-party certification involves contracts between manufacturers and certification bodies whereby prototypes and samples collected during production are tested against specific standards. Compliant products will bear the appropriate certification marks. Non-compliant products would be discarded. Here, the conformity assessment activity is performed by a person or body[27] that is independent of the person or organization that provides the object and has no user interest in the object (Woodley 2016).

Accreditation and International Mutual Recognition

One of the fundamental objectives pursued by private sector participants in international standardization activities is "one standard, one test, one certification, applicable everywhere." This objective has been driving efforts over the past 70 years, first to "build bridges" between national, regional and continental systems, and then to make concerted efforts to migrate from national to international standards. These efforts were not planned or executed top-down. Rather, they followed market trends toward globalization and longer, more complex supply chains.

In order for products or laboratory test results to be recognized not only in the country where they originate but internationally, a system made up of a series of international mutual recognition agreements administered by multilateral bodies has been established around the world. Organizations such as the International Accreditation Forum,[28] the International Laboratory Accreditation Cooperation,[29] the Asia Pacific Laboratory Accreditation[30] and the Inter-American Accreditation Cooperation[31] audit their members regularly. They provide an assurance to government, business and the consumer that organizations providing certification to a standard have the required competence and impartiality to do so as evidenced by the fulfilment of international standards and requirements.

Most national accreditation bodies belong to these international organizations. Periodically, they invite peers from other countries to visit their facilities and audit their staff competencies, operations, quality management systems and complaint-resolution processes. A determination can then be made as to whether service levels match international accreditation standards. A successful audit confers a status of accreditation to national accreditation bodies. As a result, it will be easier for products certified under a national accreditation body to be accepted in another country without having to go through duplicative certification processes elsewhere. Accreditation helps to underpin the credibility and performance of goods and services (International Accreditation Forum 2019).

27 The SDOs and conformity assessment bodies accredited by the SCC can be viewed at https://researchmoneyinc.com/wp-content/uploads/2018/01/SCC_PRE_Scale-Up-Through-Standards-Setting_2018-04-06.pdf.

28 See https://iaf.nu/en/home.

29 See https://ilac.org.

30 See www.apac-accreditation.org.

31 See www.iaac.org.mx/index.php/en/.

In the context of compliance with mandatory privacy standards, having mutual recognition agreements in place between Canada and other jurisdictions would be highly beneficial for Canadian firms. It would allow Canadian firms applying internationally recognized standards to comply with other legislation without having to undertake duplicative certifications or audits when exporting products or services abroad. A privacy RAAB could spur the adoption of international privacy compliance standards in Canada and encourage the creation of international mutual recognition agreements with other trading partners. CETA allows for mutual recognition agreements to be negotiated and cemented between SCC and EA, the SCC's European counterpart. An equivalency agreement between the Canadian privacy framework and the GDPR could be envisaged.

Standardization in the ICT and Digital Governance Sectors

When it comes to the ICT sector, standards-setting activities can only be described as extraordinarily complex, opaque, evolutionary, bottom-up and unpredictable. A number of factors led to the development of new models for standards and specifications setting operating in parallel to traditional SDOs. The author is referring here to consortia standards, specifications setting and open-source software collaboratives. However, one can see the emergence of a more coherent approach to standardization in the emerging digital governance sector, which requires ongoing communication and transparency to be seen as credible by citizens, customers and regulators.

ICT Sector

In its infancy, the ICT sector (encompassing telegraphs, telephones, cables, radio and spectrum management) followed the same path as other industries and relied on the traditional standards development model. Organizations such as the ITU began to set international interoperability standards for telegraphs in the 1860s, which allowed for the development of a global communications framework. The same path was used to support the deployment of more recent ICT technologies such as the transistor, television, electronic devices and even satellite telecommunications.

However, with digitization in the 1970s came about new approaches for setting standards and specifications to achieve interoperability. By digitization, the author is referring to the advent of software, the internet and products such as computers and handheld devices that allow for electronic information to be accessed, stored, transmitted and manipulated electronically. The requirements for this sector were different and unique when compared to other sectors of the economy. The explosive growth of the World Wide Web, intense competition between organizations for market share, rapid product development and obsolescence cycles, increased complexity of products, intense battles to incorporate essential patents into specifications, lack of regulatory oversight (in part because the deployment of these technologies did not appear to generate additional health and safety risks for consumers), and the opportunity to launch new products globally created significant demand for new standards and specifications. However, the standards absolutely needed to be developed at a pace and a level of complexity that the established SDOs just could not meet (Updegrove 2007).

ICT Standards Consortia

Starting in the 1980s, standards consortia organizations began to appear in addition to the established SDOs already operating in that space, culminating in more than 435 ICT consortia-developing standards and technical specifications bodies between 1998 and 2012. Approximately 60 percent of standards and specifications covering the ICT sector were created by consortia, including well-recognized interoperability standards such as universal serial bus drives, digital video discs, the Blu-ray optical disc format, Hypertext Markup Language, ultra-high definition, Extensible Markup Language, Musical Instrument Digital Interface and peripheral component interconnect express. Established international SDOs also played an important role in developing other standards such as Wi-Fi, short message service, fourth-generation technologies and moving picture experts group audio layer-3 (Biddle et al. 2012).

To give an idea of the scale of the effort required to establish interoperability frameworks to support the commercialization of new products, Brad Biddle and other ICT standardization experts estimated in 2012 that at least 251 interoperability standards are embedded in a modern laptop computer, with many hundreds more needed for communicating information from one device to another through the internet.

Standards consortia played an essential role in the rapid deployment of the personal computer, computer software and the internet. Market participants, often frustrated at the slow pace of development in established SDOs, created individual consortia to "create the standard" in new fields when new technologies or processes were ready for market. Tim Pohlmann (2014, 37), who undertook a comprehensive survey of the evolution of ICT sector consortia in 2012, noted that although they differ widely in terms of organizational structures, policies, bylaws and purpose, consortia are generally smaller in terms of members than traditional SDOs, frequently follow only one purpose of business, are often hierarchical in their decision-making structures and are, in many cases, organized in tiered membership structures.

Biddle et al. (2012) identified the following types of consortia operating in the ICT sector.

- **Single-promoter specifications:** These are generally used by individual companies to make a specification available for industry adoption, including a covenant not to assert necessary claims.
- **Contractual consortia:** These are groups in which multiple partners jointly develop a specification. Partners enter into promoters' agreements that address licensing commitments in necessary claims. They can also extend agreements with contributors and adopters once the specification is designed.
- **Incorporated consortia:** These are organized around multilateral contracts establishing membership or participation agreements requiring members to abide by the obligations set forth by the consortium bylaws and IP rights policies in exchange for access to the specifications or design guidelines and the benefits of the licensing commitments that accompany them. Incorporated consortia have various levels of membership. Benefits include the right to own and license trademarks and administer certification programs.
- **Hybrid model:** This incorporates elements of contractual and incorporated consortia.

Because consortia are generally tied to one technology, they are more sensitive to technology and market shocks and tend to have shorter lives than traditional SDOs. This explains why most of the consortia created in the 1990s have been dissolved or amalgamated with others. Technical committees are generally short-lived and membership fluctuates greatly from one year to the next. As their main objective is to facilitate the commercialization of new products, few consortia followed the WTO's six principles, such as fostering broad public participation.

As mentioned in the introduction, it is very clear that the development of new platforms and technologies such as IoT devices and wearables used in the rapidly growing telehealth-care and wellness sector will require ongoing privacy management to keep users safe from harms. Somehow, privacy requirements will have to be "baked in" these devices just like cybersecurity standards are now finding their way into IoT and industrial IoT devices (Digital Governance Standards Institute 2022). A Canadian privacy RAAB will probably need to articulate a view on how to review, manage and possibly adopt privacy standards and technical specifications issued by consortia organizations to cover these technologies.

Open-Source Software Development

The entire edifice of digitization is based on software development and coding. As this new sector appeared, so did new approaches to draft, test and ensure new products' interoperability from software to code language and apps. Although traditional SDOs are still used to generate rules for broad applications such as cybersecurity management systems or cloud computing, by and large, software developers shunned traditional SDOs and standards/specifications consortia in favour of open-source software platforms. Large organizations such as Microsoft, which relied heavily on traditional SDOs to ensure interoperability, testing and certification of products such as cloud computing in the early 2000s, now rely on development platforms such as GitHub to host and review code and build software with a community that grew from 24 million developers in 2019 to more than 100 million developers early in 2023 (Dohmke 2023). But like consortia, open-source development platforms are simply not designed to solicit broad public participation for making choices between various approaches or to integrate social or other considerations as a new product is being designed.

Rather, when a project is assigned to open-software development platforms, fundamental questions

as to the "whether," the "what," the "why" and the possible alternatives to an approach have already been answered. Participants are invited to work together to fix bugs and to help with the "how," such as product design, outreach and marketing, to ensure new projects actually work as intended when launched. This raises accountability and responsibility issues when software may impact the health, safety and security of users.

There are also a number of not-for-profit and charitable organizations supporting the open-source software movement, such as the Linux Foundation. Most of these organizations are promoting the free use of software and operating languages although some, such as the Free Software Foundation, are aimed at the development and use of free software for "having control over the technology we use in our homes, schools, and businesses, where computers work for our individual and communal benefit, not for proprietary software companies or governments who might seek to restrict and monitor us."[32]

Digital Governance

Thousands of global technical standards were necessary to support the creation of the internet and the World Wide Web. One can easily imagine that a large number of standards will also be required to manage the myriad of digital governance issues created by the deployment of the internet and global platforms. A cursory review reveals a dozen major international standards bodies and consortia involved in developing standards and specifications to manage interrelated, value-laden issues such as privacy, ethics, trust and fairness.

In 1987, the ISO and the IEC established Joint Technical Committee (JTC) 1 by merging ISO Technical Committee 97 (information technology) and IEC Technical Committee 83 (information technology equipment). JTC 1 is seen by many as the leading body making progress in coordinating activities for data management, big data and artificial intelligence (AI). Its purpose is to develop, maintain and promote standards in the fields of IT and ICT. Since its creation, JTC 1 has published more than 3,200 standards and publicly available specifications covering a wide array of subjects including programming languages, interconnection of IT equipment, user interfaces, cloud computing, cybersecurity, data security, big data, data management and interchange, and more recently, the IoT and AI.[33]

It manages a substantive proportion of the two organizations' standards catalogue (ISO maintains more than 20,000 standards and IEC more than 10,000). JTC 1 operates through a matrix of subcommittees, working groups and advisory groups that are connected to more than 100 liaison bodies. For example, Subcommittee 42 focuses on big data and AI through four working groups (WGs):

- WG 1: Foundational standards (concepts and terminology);
- WG 2: Big data (overview, definitions, reference architecture);
- WG 3: Trustworthiness (biases in AI systems, overview, robustness of neural networks); and
- WG 4: Use cases and applications.

The Institute of Electrical and Electronics Engineers Standards Association (IEEE SA) has been active in the ICT sector for decades through a large number of technical standards for electronic products, such as the ethernet and Wi-Fi as well as software engineering management. In 2017, IEEE had more than 1,100 active standards, with more than 600 standards under development. Regarding big data analytics, IEEE launched in 2017 a global consultation and outreach initiative called Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. IEEE is now spearheading the development of 15 ethical AI standards under its 7000 series ranging from algorithmic bias consideration and managing privacy when developing AI systems to automated facial analysis technology with the input of more than 2,000 participants.[34]

IEEE SA also launched the development of an Ethics Certification Program for Autonomous and Intelligent Systems, which represents the first attempt to design and deploy an international compliance mechanism toward ethical AI standards. If successful, the new program

32 See www.fsf.org/about/; https://opensource.com/resources/organizations.

33 See https://jtc1info.org/.

34 See https://ethicsinaction.ieee.org/.

could provide certification for algorithmic bias, accountability and transparency.[35]

In 2018, IEEE led the creation of OCEANIS, the Open Community for Ethics in Autonomous and Intelligent Systems, along with 15 SDOs that joined as founding members and 19 members from the private sector. It is intended to act as a high-level global forum for discussion, debate and collaboration for organizations interested in the development and use of standards to further the advancement of autonomous and intelligent systems. Its creation could spur greater collaboration and cooperation among standard-setting bodies focusing on algorithms, sensors, big data, ubiquitous networking and technologies.[36]

The ITU, the UN agency accountable for global standards covering telecommunications and ICT, is the custodian of the International Telecommunication Regulations treaty. It maintains more than 4,000 normative documents, including standards. The ITU is an active player in the development of data sharing, IoT and smart cities standards. It provides comprehensive training on AI and digital skills.[37]

The European Technology Standards Institute (ETSI) produces standards and specifications for ICT-enabled systems and is focusing on issues such as blockchain, AI, augmented reality and autonomous networks standards. ETSI has published more than 45,000 standards and specifications, which are routinely incorporated by reference in European regulations. It has an ambitious work program related to big data analytics, cybersecurity and privacy to facilitate compliance with the GDPR (ETSI 2022).

The Internet Engineering Task Force is actively engaged in standardization efforts for application programming interfaces, IoT devices, security and privacy considerations.[38]

In Canada, the CIO Strategy Council was accredited by SCC in 2018. It develops digital governance standards covering topics such as AI systems, cybersecurity, digital identity and credentials, biometrics, data governance in the health-care sector, electoral voting technologies as well as privacy and access control. In 2023, members decided to focus exclusively on digital governance and created the Digital Governance Council and the Digital Governance Standards Institute. The organization has recently received approval to submit its standards and specifications for review and recognition as international standards. As its approved standards carry both the ISO and IEC logos, the Digital Governance Standards Institute should be considered an international standards development body.

35 See https://standards.ieee.org/industry-connections/ecpais/.

36 See https://ethicsstandards.org/.

37 See www.itu.int/en/Pages/default.aspx.

38 See www7.ietf.org/topics/security/.

Works Cited

Biddle, Brad, Frank X. Curci, Timothy F. Haslach, Gary E. Marchant, Andrew Askland and Lyn Gaudet. 2012. "The Expanding Role and Importance of Standards in the Information and Communications Technology Industry." *Jurimetrics* 52 (2): 177–208. www.jstor.org/stable/23239825?seq=1#page_scan_tab_contents.

Breznitz, Dan and Michael Murphree. 2018. "Technology Standardization in the Global Economy – Implications for Canada." Standards Council of Canada Working Paper.

Canada Mortgage and Housing Corporation. 2019. "Request for Proposal for Unstructured Data Archiving Solution." Solicitation No. PR002710. March 20. https://canadabuys.canada.ca/en/tender-opportunities/award-notice/pw-19-00868243-901958.

Centre for Data Ethics and Innovation. 2021. *The roadmap to an effective AI assurance ecosystem – extended version.* Government of the United Kingdom. December 8. www.gov.uk/government/publications/the-roadmap-to-an-effective-ai-assurance-ecosystem/the-roadmap-to-an-effective-ai-assurance-ecosystem.

Committee on Conformity Assessment. 2019. "ISO/IEC 17029 – Conformity assessment: General principles and requirements for validation and verification bodies." ISO 34th Plenary Meeting, May 1–2, Nairobi, Kenya.

CSA. 1996. "Model Code for the Protection of Personal Information." National Standard of Canada. CAN/CSA Q830-96. Etobicoke, ON: CSA. March.

CSA Group. 2004. *PLUS 8300 – Making the CSA Privacy Code Work for You – A Workbook on Applying the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830) to Your Organization; PLUS 8830 – Implementing Privacy Codes of Practice – Commentary and CSA Q830:03, Model Code for the Protection of Personal Information.* www.csagroup.org/store/product/PRIVACY%20PACKAGE/.

———. 2022. *2021/2022 Annual Report – For a Safer, More Sustainable Future.* www.csagroup.org/annual-report/.

Data Transfer Project. 2018. "Data Transfer Project Overview and Fundamentals." July 20. https://datatransferproject.dev/dtp-overview.pdf.

Digital Governance Standards Institute. 2022. *CAN/CIOSC 105:2022 Cybersecurity of Industrial Internet of Things (IIoT) Devices.* Ottawa, ON: CIO Strategy Council. https://dgc-cgn.org/standards/find-a-standard/standards-in-cybersecurity/cybersecurity-iiot/.

Dohmke, Thomas. 2023. "100 million developers and counting." *GitHub* (blog), January 25. https://github.blog/2023-01-25-100-million-developers-and-counting/.

ETSI. 2022. *Technical Committee (TC) Cyber (Cybersecurity) Activity Report 2022.* www.etsi.org/committee-activity/activity-report-cyber?highlight=WyJwcml2YWN5Il0=.

European Commission. 2021. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." COM(2021) 206 final. www.europarl.europa.eu/meetdocs/2014_2019/plmrep/AUTRES_INSTITUTIONS/COMM/COM/2021/06-02/COM_COM20210206_EN.pdf.

European Delegation to Canada. 2020. "Study on Standards." EU-Canada Policy Dialogues Support Facility. August.

Fadrique, Laura, Amethyst Kuang, Larissa Ugaya Mazza and Plinio Pelegrini Morita. 2020. *Rethinking Privacy Agreements.* Etobicoke, ON: CSA Group. March. www.csagroup.org/article/research/rethinking-privacy-agreements/.

Girard, Michel. 2018. "Helping Canadian Companies Scale Up Through Standards Setting." Keynote address presented at the Spring 2018 RE$EARCH MONEY Conference: Breaking Through the Status Quo – Scaling Canada's Innovation Game. April. www.scc.ca/en/news-events/news/2018/helping-canadian-companies-scale-through-standards-setting.

———. 2019. *Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter.* CIGI Paper No. 209. Waterloo, ON: CIGI. www.cigionline.org/publications/big-data-analytics-need-standards-thrive-what-standards-are-and-why-they-matter/.

Harish, Ajay. 2022. "When NASA Lost a Spacecraft Due to a Metric Math Mistake." *SimScale* (blog), October 17. www.simscale.com/blog/nasa-mars-climate-orbiter-metric/.

International Accreditation Forum. 2019. "The IAF Multilateral Recognition Arrangement (MLA)." Chelsea, QC: IAF Secretariat. https://stage.iaf.nu/wp-content/uploads/2021/05/IAF_MLA_0112-Secretariat-Comments-13102019.pdf.

ISO. 2019. "ISO/IEC Guide 59:2019 ISO and IEC recommended practices for standardization by national bodies." August. www.iso.org/standard/71917.html.

———. 2023. "ISO 31700-1:2023 Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements." January. www.iso.org/standard/84977.html.

ISO/IEC. 2014. *Using and referencing ISO and IEC standards to support public policy*. Geneva, Switzerland: ISO. www.iso.org/publication/PUB100358.html.

Jennings, Hayley. 2018. "Facebook, Twitter, Google and Microsoft Team Up on New Data Project." PR News, July 20. www.prnewsonline.com/twitter-facebook-google-microsoft-team-up-on-new-data-project.

McKean, Ross, Ewa Kurowska-Tober, Heidi Waem and Rachel de Souza. 2023. *DLA Piper GDPR Fines and Data Breach Survey: January 2023*. DLA Piper. www.dlapiper.com/en/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023.

National Institute of Standards and Technology. 2023. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. January.

Pohlmann, Tim. 2014. "The Evolution of ICT Standards Consortia." *DigiWorld Economic Journal* 95 (3): 17–40.

Ray, Siladitya. 2022. "Apple Will Have To Switch To USB-C Chargers For iPhones From 2024 After EU Vote." *Forbes*, October 4. www.forbes.com/sites/siladityaray/2022/10/04/apple-will-have-to-switch-to-usb-c-chargers-for-iphones-from-2024-after-eu-vote/?sh=66ba0fb138c3.

SCC. 2017. *Canadian Standards Development Program Overview*. Ottawa, ON: SCC. www.scc.ca/en/about-scc/publications/requirements-and-procedures-accreditation/canadian-standards-development-program-overview.

———. 2019a. *Canadian Standards Development Requirements & Guidance – Accreditation of Standards Development Organizations*. Ottawa, ON: SCC. June 13. www.scc.ca/en/system/files/publications/SIRB_RG_SDO-Accreditation_v4_2021-03-04.pdf.

———. 2019b. *Canadian Standards Development National Technical Specifications*. Ottawa, ON: SCC. August 2. www.scc.ca/en/about-scc/publications/general/national-technical-specifications.

———. 2019c. *Annual Report 2018–2019: Delivering Value Together*. Ottawa, ON: SCC. August 21. www.scc.ca/en/about-scc/publications/documents-du-ccn/rapports-annuels/annual-report-2018-2019-delivering-value-together.

———. 2020. "Understanding GDPR: The role of standards in compliance." Ottawa, ON: SCC. November 5. www.scc.ca/en/system/files/publications/SCC_GDPR_Report_EN.pdf.

———. 2021. *Aging. Flexibility. Compassion. 2020–2021 Annual Report*. Ottawa, ON: SCC. November 30. www.scc.ca/en/about-scc/publications/corporate-documents/annual-reports/annual-report-2020-2021.

———. 2022. *Moving Forward Together. 2021–2022 Annual Report*. Ottawa, ON: SCC. October 12. www.scc.ca/en/about-scc/publications/corporate-documents/annual-reports/moving-forward-together-2021-2022-annual-report.

UK. 2021. *National AI Strategy*. Presented to Parliament by the Secretary of State for Digital, Culture, Media and Sport by Command of Her Majesty. Command Paper 525. September. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf.

Updegrove, Andrew. 2007. "ICT Standard setting today: A system under stress." *First Monday* 12 (6). https://doi.org/10.5210/fm.v12i6.1911.

Wijkström, Erik and Devin McDaniels. 2013. "International Standards and the WTO TBT Agreement: Improving Governance for Regulatory Alignment." World Trade Organization Economic Research and Statistics Division. Staff Working Paper ERSD. 2013-06. April 25. www.wto.org/english/res_e/reser_e/ersd201306_e.pdf.

Woodley, Cynthia D. 2016. "First, Second and Third Party: What Does it Mean in Certification of Persons?" *Professional Testing* (blog), September 28. www.proftesting.com/blog/2016/09/28/first-second-and-third-party/.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline