THE MISSING LINK

Why Government Bodies Must Consolidate Cybersecurity and Privacy Regulations

Author:
Abhay B Bhingradia
Analyst, Security Operations Center

As cybersecurity threats continue to surge and consumers demand stronger data protections, it might seem logical to expect clear, comprehensive, and centralized guidance from government agencies. After all, organizations such as the Office of the Privacy Commissioner of Canada, the U.S. Federal Trade Commission, and various European data-protection authorities are entrusted with enforcing data-protection and cybersecurity requirements. Yet despite the proliferation of laws and the growing urgency of these threats, no single, authoritative repository of these mandates exists within most jurisdictions. This paper argues that by failing to provide an official, consolidated index of cybersecurity and privacy regulations for their respective domains, government bodies have left businesses—and the public—to piece together a bewildering patchwork. The result is not just confusion and compliance fatigue but also heightened security and privacy risks for everyone involved.

To help fill this gap, we have compiled our own **master list** of key cybersecurity and privacy requirements across several jurisdictions and industries, which readers can access as an **attached supplementary resource**. This list serves as a demonstration of both the extent of current regulations and the glaring absence of a government-provided equivalent.

In Canada alone, organizations must contend with an array of federal, provincial, and sector-specific privacy laws. At the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies broadly, while certain provinces—such as Alberta, British Columbia, and Quebec—have their own private-sector privacy acts or modernized rules. Healthcare entities operate under additional statutes, such as Ontario's Personal Health Information Protection Act (PHIPA), and many industries also face specialized cybersecurity mandates, for instance under Bill C-26, which focuses on critical infrastructure security.

A similar dynamic occurs in the United States, where federal laws like HIPAA, FISMA, or CIRCIA overlap with state-level privacy regimes, including the California Consumer Privacy Act (CCPA) and the ever-evolving patchwork of other state statutes. In the European Union, the GDPR, NIS 2, and the EU Cybersecurity Act are key pillars, yet multiple sector-focused directives and country-specific implementations make compliance a significant challenge.

Given this tangled web of obligations, businesses—especially smaller ones—struggle to even identify which laws govern their data or systems, much less implement the myriad processes required to stay compliant. They frequently turn to consultants or build homegrown catalogs of references in spreadsheets. Although these efforts may be laudable, they underscore a question that is all too often asked: **If the government has the authority to regulate and enforce, why can't it offer a comprehensive, centralized list of all applicable regulations in the first place?**

The **Office of the Privacy Commissioner of Canada** (OPC) is a prime example of an agency with a mandate to protect privacy rights yet provides limited consolidated guidance. Its website features helpful documents and FAQs on PIPEDA or specific privacy issues, but it does not offer a regularly updated master reference that covers the full range of federal and provincial laws, let alone associated cybersecurity mandates. Businesses operating across multiple provinces must check the OPC's guidance, consult provincial commissioners' websites, and review underlying legislation themselves. The lack of coordination between federal and provincial bodies exacerbates the confusion, leaving many to piece together key rules from disparate sources.

In the United States, government agencies such as the Federal Trade Commission (FTC) or the Office for Civil Rights at the Department of Health and Human Services (for HIPAA enforcement) exhibit a similar siloed approach. They tend to focus on their own regulatory realms, offering partial references at best. Given the multi-layered nature of American governance—where states enact their own privacy and cybersecurity laws—no single federal authority publishes a nationwide compilation of cybersecurity or data privacy statutes. The result is that large corporations and small businesses alike must rely on private consultancies or painstaking internal research.

Meanwhile, European data-protection authorities, along with the European Data Protection Board (EDPB), remain focused on the enforcement and interpretation of the GDPR, providing guidance but not a unified resource that also tracks developments like NIS 2, eIDAS, or the EU Cybersecurity Act. Each legislative piece tends to be treated separately, leaving organizations to cross-reference regulations on their own.

The fallout of this patchwork approach is significant. First, organizations face **elevated compliance costs**. Rather than consult a single, reliable government guide, they must sift through multiple websites, pay for legal opinions, or invest in proprietary solutions that aggregate relevant legislation. This is especially challenging for small and medium-sized enterprises, which often lack the budget for a full-time legal or compliance team.

Second, **risk of non-compliance rises** when businesses fail to discover new or changed rules. Many are unaware that they have to meet certain provincial standards in Canada, for instance, or that specific U.S. states impose additional requirements beyond what they have already satisfied at the federal level. Ironically, the government bodies that levy penalties also fail to provide the clarity that might prevent such violations.

Third, **public trust in regulatory agencies** can erode when people realize how fragmented the system is. If agencies are truly committed to protecting consumer rights and ensuring robust cybersecurity, it stands to reason they would facilitate access to the very laws they enforce. By not offering a centralized resource, these bodies appear either uncoordinated or unconcerned about the administrative burdens their mandates impose on regulated entities.

A **government-published** list of cybersecurity and privacy obligations, regularly updated and thorough in scope, would provide immense value to stakeholders. Businesses could better anticipate their responsibilities, reduce the time and cost of compliance, and more effectively safeguard their systems and data. Consumers and advocacy groups could also verify which rules are in force, thereby strengthening public confidence in governmental oversight. Such a list would bring immediate transparency and potentially reduce disputes by clarifying regulatory requirements.

Yet, despite these clear benefits, the absence of official, centralized compilations remains the status quo in almost every major jurisdiction. This gap is precisely why we have undertaken the initiative to create and share our own master list—drawing from federal, provincial, and regional sources in Canada, parallel laws in the United States, directives in the European Union, and certain global standards such as ISO 27001 and IEC 62443. While it may not have the legal authority of a government publication, it serves as a demonstration of how straightforward access to this information could be—if only governments were willing to invest the effort.

This paper is accompanied by a separate document—referred to here as the **Master List**—which the reader can find attached at the end of this file or as a downloadable link if this paper is distributed electronically. It consolidates prominent legislation (e.g., PIPEDA, FISMA, GDPR), industry-accepted standards (e.g., ISO 27001, IEC 62443), and sector-specific mandates (e.g., ICAO annexes for aviation, HIPAA for healthcare), organized by both **jurisdiction** and **industry sector**.

The Master List is neither exhaustive nor officially endorsed by any government agency. Nonetheless, it highlights the kinds of comprehensive references that would prove invaluable if compiled and maintained by regulatory authorities themselves.

Government agencies like the Office of the Privacy Commissioner of Canada should seize the opportunity to streamline compliance by providing an authoritative, consolidated index of laws and standards within their purview. They could do so in partnership with provincial commissioners, ensuring the centralized resource covers not only federal legislation but also the provincial and territorial rules that add complexity to the national picture. If the mandate of a single agency is too narrow, then inter-agency collaboration becomes essential. At the very least, the relevant bodies should cross-link official websites and unify guidance, so organizations are not forced into a scavenger hunt for relevant statutes.

A similar argument can be made for U.S. agencies or for EU-level bodies responsible for GDPR enforcement, cybersecurity directives, and various other regulations. Piecemeal publications of guidance and case decisions have their value, but they do not replace the basic need for a clear, up-to-date index of all binding rules. Until such an index exists, businesses will have little choice but to rely on private consultants or community-driven lists like the one attached here—solutions that, while practical, often prove costly and, ironically, put more power in the hands of for-profit entities than in the public sector itself.

Cybersecurity and privacy laws are indispensable in today's digital world, but they are often complex, overlapping, and scattered across multiple levels of government. The agencies that enforce these laws can significantly reduce compliance burdens and strengthen security by offering a definitive, centralized list of regulations. Yet so far, few—if any—have stepped up to provide such a service.

By distributing this paper and our attached master list, we aim to highlight both the pressing need for centralized guidance and the shortcomings of current government-driven approaches. While we recognize that regulatory nuances can be intricate, that is precisely why government-sponsored clarity is so badly needed. Without it, the system remains inefficient, confusing, and potentially less secure than it ought to be—an outcome that ultimately harms not just businesses and citizens, but the credibility of the agencies themselves. It is time for bodies like the Office of the Privacy Commissioner of Canada to move beyond narrow, fragmented advisories and deliver the user-friendly, comprehensive reference that organizations and the public have long deserved.

References:

1. **Office of the Privacy Commissioner of Canada (OPC).** (n.d.).
   Retrieved from https://www.priv.gc.ca/en/
   (Covers PIPEDA oversight and related federal privacy guidance.)
2. **Personal Information Protection and Electronic Documents Act (PIPEDA).** (2000).
   S.C. 2000, c. 5. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/P-8.6/
   (Governs private-sector privacy rules federally in Canada.)
3. **Bill C-26: An Act Respecting Cyber Security (Critical Infrastructure).** (2022).
   Parliament of Canada. Retrieved from https://www.parl.ca/LegisInfo/BillDetails.aspx?billId=11815586
   (Proposes cybersecurity measures for critical infrastructure in Canada.)
4. **Provincial Privacy Legislation**
   a. **Alberta**: Personal Information Protection Act (PIPA).
   b. **British Columbia**: Personal Information Protection Act (PIPA).
   c. **Quebec**: Act respecting the protection of personal information in the private sector (including Bill 64 updates).
5. **Personal Health Information Protection Act (PHIPA).** (2004).
   S.O. 2004, c. 3, Sched. A (Ontario). Retrieved from https://www.ontario.ca/laws/statute/04p03
   (Sets rules for handling health records in Ontario.)
6. **United States Department of Health & Human Services (HHS).** (n.d.).
   Retrieved from https://www.hhs.gov/
   (Includes HIPAA privacy and security rule enforcement.)
7. **Health Insurance Portability and Accountability Act (HIPAA).** (1996).
   Pub. L. No. 104-191. Retrieved from https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm
8. **Federal Information Security Modernization Act (FISMA).** (2014).
   Pub. L. No. 113-283. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521
9. **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).** (2022).
   Division Y of the Consolidated Appropriations Act, 2022. Retrieved from https://www.congress.gov/bill/117th-congress/house-bill/2471/text
10. **California Consumer Privacy Act (CCPA).** (2018).
    Cal. Civ. Code § 1798.100 et seq. Retrieved from https://oag.ca.gov/privacy/ccpa
11. **Federal Trade Commission (FTC).** (n.d.).
    Retrieved from https://www.ftc.gov/
    (Responsible for enforcing federal consumer protection and privacy laws in the U.S.)
12. **European Commission: Data Protection.** (n.d.).
    Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en
    (Includes official documents and guidance on the GDPR, among other EU frameworks.)
13. **Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).** (2016).
    Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj
14. **Directive (EU) 2016/1148 (Network and Information Systems Directive - NIS).** (2016).
    Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj
15. **EU Cybersecurity Act (Regulation (EU) 2019/881).** (2019).
    Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/2019/881/oj
16. **European Data Protection Board (EDPB).** (n.d.).
    Retrieved from https://edpb.europa.eu/
    (Oversees consistent application of GDPR across EU member states.)
17. **International Civil Aviation Organization (ICAO).** (n.d.).
    Retrieved from https://www.icao.int/
    (Includes annexes and standards for aviation security and other regulatory frameworks.)
18. **ISO 27001: Information Security Management Systems.** (2013/2022).
    International Organization for Standardization (ISO). Retrieved from https://www.iso.org/isoiec-27001-information-security.html
19. **IEC 62443: Industrial communication networks – Network and system security.** (n.d.).
    International Electrotechnical Commission (IEC). Retrieved from https://webstore.iec.ch/searchform&q=62443