Deloitte. Legal

Client Alert: New Cyber & Privacy Laws, New Risks, New Compliance Requirements

The federal government recently introduced not one – but two – new bills that will overhaul Canadian cybersecurity and privacy law if passed. While these are exciting developments for privacy practitioners, the new legislation creates a host of obligations (which raise important questions) for critical infrastructure (CI) firms, corporations that collect/use/disclose personal information, and private sector organizations that develop and employ artificial intelligence (AI).

Bill C-26, an *Act Respecting Cyber Security* (ARCS), would give the federal government broad powers over protecting critical infrastructure sectors from cybersecurity threats.

- The first part of ARCS is specific to telecommunications companies and would authorize the government to order the approval, rejection, or removal of systems and services deemed threats to national cybersecurity interests. The government could also keep such orders secret (e.g., to limit the disclosure of a telecom's cyber vulnerabilities).
- The second part of ARCS sets out significant new cybersecurity planning and response obligations for federally regulated CI sectors (i.e., finance, transport, telecoms, energy). One of these obligations includes the immediate reporting of cybersecurity incidents to the Communications Security Establishment (CSE).
    - Failure to meet these obligations and remediate violations could result in massive fines under the proposed law, including $1,000,000/day for individuals and $15,000,000/day for organizations.

Bill C-27 is an expanded and updated version of the *Digital Charter Implementation Act* (DCIA), which originally was tabled in 2020 but did not pass before last year's federal election. DCIA is broken into three parts addressing data privacy obligations, administrative appeals, and AI rules:

- The first part would enact the *Consumer Privacy Protection Act* (CPPA), the federal government's second attempt at a new private sector privacy law meant to modernize personal information collection, use, and disclosure in an ever-changing digital landscape. Obligations include:
    - Requiring transparent and easily accessible privacy policies for consumers;
    - Designating privacy resources and implementing a comprehensive management program;
    - Expanding the federal privacy commissioner's (OPC) authority to investigate complaints and recommend privacy program changes, along with monetary penalties where appropriate - $10,000,000 or 3% of a company's global gross revenue for certain contraventions; $25,000,000 or 5% of global gross revenue for more serious offences (in both cases, whichever is higher);
    - New rules when dealing with the personal information of minors; and
    - Providing a private right of action to individuals.

- The second part would enact a new administrative tribunal under the ***Personal Information and Data Protection Tribunal Act***, which would hear appeals from, and potentially impose administrative monetary fines recommended by, the OPC.
- The third part would enact the ***Artificial Intelligence and Data Act*** and be meant to regulate international and interprovincial trade and commerce in AI systems. Specifically,
    - The new law will create several AI-related offences and violations, including improper use of personal information; being reckless with AI likely to cause serious harm to individuals or substantial damage to property; and using AI to commit fraud.
    - Penalties can be up to $25,000,000 or 5% of global gross revenue for organizations, and for individuals is discretionary with up to five years' imprisonment.
    - Given the number of definitions and principles that remain outstanding (likely to be cleared up in regulations), organizations may look to the European Union's ***AI Act*** for guidance (based on past legislative practice in Canada; for example, Parliament previously used the EU AI Act's four groups of AI risk classification in the Directive on Automated Decision Making).

Olivier Bonne
Direct Line: 514-390-1688 |Cell: 438-458-1273
obonne@deloitte.ca | deloitte.ca

Hélène Deschamps Marquis
Direct Line: 514-393-8300 |Cell: 514-497-9240
hdeschampsmarquis@deloittelegal.ca | deloittelegal.ca