CCLS Education Sub-Committee Education Week Webinar

Title	***Privacy, what's new on the horizon…***
Program Summary	This informative webinar focused on Quebec's new privacy law (Bill 64) and proposed changes to Canada's federal privacy legislation (Bill C-27). The panelists discussed the legal and regulatory impacts of these changes and best practices for implementing a compliant privacy program.
Legal Disclaimer	The webinar and this summary document provide general information on legal and related matters and should not be relied upon as legal advice. If you require legal advice, you should retain qualified legal professionals to advise you in the context of your particular circumstances.
Program Date	Thursday, December 8th, 2022
Participants and Bios	1. Facilitator: Shaun McIver, CEO, Vayle (bio) shaun.mciver@vayle.io | (416)-419-6445 2. Julie Himo, Partner, Torys LLP (bio) jhimo@torys.com | (514)-868-5634 3. Kris Klein, nNovation LLP (bio) kklein@nnovation.com | (613) 882-2909
Participant Bios	Thursday, December 8th, 2022
Reference Links	**IAPP Canada:** • Canada Dashboard Digest (incl. Kris Klein articles) **Shaun McIver articles and Reference Materials:** • CPO Magazine: Quebec's new privacy law regime was just adopted. Are you ready? (op-ed) • ITWorld Canada: 7 Steps to undertaking a Privacy Impact Assessment (op-ed) **Julie Himo/ Torys LLP Articles and Reference Materials:** • Privacy in Québec: recent developments and takeaways for businesses • Bill 64's adoption confirms overhaul of Québec private sector privacy law

	• Automated decision-making: what Québec's Bill 64 reforms mean for business • Director and officer liability for cybersecurity breaches in Canada and the U.S. • Challenges to privilege over cybersecurity investigations: Cross-border litigation trends
Program Objectives	1. ***Understand*** *the changing world of privacy more broadly across the public and private sectors.* 2. ***Identify*** *essential compliance requirements for Bill 64 and proposed Bill C-27 and potential risks for IIROC organizations that fail to comply.* 3. ***Define*** *practical steps IIROC member organizations should undertake to enhance your privacy program, irrespective of existing or pending regulations.*

Q1	***Please provide a general overview of Bill 64 and proposed C-27.***
Bill 64	• Bill 64 was adopted in September 2021 and is coming into force in phases over the course of 2022, 2023, and 2024. It is the first Canadian push towards a GDPR-like framework. • Bill 64 updates and modernizes both the public and the private sector privacy legislation in Quebec. It forces organizations that handle Quebecers' personal information ("PI") to review their practices and align with the new requirements. It applies to organizations offering services and/or collecting or using the PI of Québec based individuals even if the systems and the organization are located outside of Québec and irrespective of the organization's general regulatory framework, and it applies to federally regulated companies unless clear conflict with PIPEDA/CPPA/other federal legislation. • Key new obligations imposed by Bill 64: - The requirement to have a privacy officer, i.e. by default, the person exercising the highest authority in the organization unless delegated to someone else (Sept 2022) - Privacy framework (Sept 2023) - requiring organizations to establish and implement governance policies and practices that must be proportionate to the nature and extent of the organization's activities; organizations collecting PI through technological means must publish a confidentiality policy on their website - Breach notification requirements (Sept 2022) – introducing reporting obligation of a "confidentiality incident" involving PI for

	incidents presenting a risk of serious harm to individuals. Notify affected individuals and report to CAI. - Incident registration requirements (Sept 2022), including administrative penalties (up to $10M or 2% of revenues) and fines for non-compliance (up to $25M or 4% of revenues). - Privacy impact assessment (“PIA”) requirement (Sept 2023) - Cross-border transfer requirement (Sept 2023) - Mitigation and remediation requirements for confidentiality incidents also subject to AMPs and fines mentioned above. - Retention and processing outsourcing requirements (Sept 2023)
Bill C-27	• The Digital Charter Act (Bill C-27) has been introduced to create a Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act. • Canada’s federal privacy law currently applies to ‘federal works, undertakings and businesses’ as will CPPA. • The federal law applies within provincial jurisdiction if the province has not passed its own privacy law, which is substantially similar; currently, this includes Quebec, Alberta and British Columbia. • The federal privacy law does not address the privacy of employees of companies unless the organization is a federal work or undertaking. • CPPA will, however, expressly apply to interprovincial or international data flows so that it may have a concurrent application with provincial privacy laws.

Q2	***What is at stake for organizations that fail to comply?***
Bill 64	• Enforcement provisions that include administrative sanctions of up to $10M or 2% worldwide turnover, whichever is greater; penal offences and penalties for violations of up to $25M or 4% worldwide turnover; and that recognize the Court’s authority to sanction an unlawful infringement with punitive damages of not less than $1000 – one of few Quebec laws to provide for either punitive damages or minimum damages
Bill C-27	• Fines will range under CPPA up to 3% of global revenue for administrative monetary penalties and up to 5% of global revenue for egregious or criminal violations. • Additionally, the Office of the Privacy Commissioner (OPC) of Canada will be given order-making powers, moving away from the traditional ombudsperson role but subject to approval and review by the new Personal Information and Data Protection Tribunal.

<table>
<tr><th>Q3</th><th>What types of information are covered under these new privacy laws (i.e., personal and sensitive information)?</th></tr>
<tr><td>Bill 64</td><td>Personal information under Bill 64 means “any information which relates to a natural person and allows that person to be identified.” This means, practically speaking, any information that is directly or indirectly linkable to a person, which can include education information, financial and employment data, and IP address, among others.
Sensitive personal information under Bill 64 includes medical data, biometric data, ethnicity, religion, or otherwise intimate information – these are afforded a higher level of protection that personal information.
Personal information may become sensitive if the context of its use or communication naturally entails a high level of reasonable expectation of privacy.</td></tr>
<tr><td>Bill C-27</td><td>Personal Information keeps the same definition as in PIPEDA. It is “any information about an identifiable individual.”
The CPPA expressly states that the personal information of minors is to be considered as sensitive.</td></tr>
<tr><td>Examples</td><td>Scenarios where IIROC member organizations may be processing personal or sensitive information include: (1) capturing KYC via print or digital forms, (ii) “find an advisor” tools on a website that request location data, (ii) marketing forms used for lead generation, chatbots, etc., (iv) self-service sites to activate and manage accounts, (v) portfolio management portals, and (vi) general HR information.</td></tr>
</table>

<table>
<tr><th>Q4</th><th>What is a “privacy program,” as defined under Bill 64 and Bill C-27, and what must organizations have in place to comply?</th></tr>
<tr><td>Bill 64</td><td>Under Bill 64, organizations must have key policies in place regarding the collection, use, disclosure, access, correction, disposal and retention of personal information, as well as the responsible use of information, access to information and a complaint process regarding non-compliance.
Bill 64 creates the obligation to designate a Privacy Officer (“PO”) – this requirement came into force in September 2022. Under Bill 64, the person “exercising the highest authority” in the organization is vested with the accountability for ensuring the organization’s privacy compliance. This function can be delegated to another person while keeping accountability with the person of the highest authority.
There are some specific duties that a PO must discharge, including reviewing PIAs, assessing risk in the case of a data breach, receiving information about the violation of the Act, and responding to individual rights requests.</td></tr>
<tr><td>Bill C-27</td><td>Section 9 mandates organizations maintain a privacy management program.
For both the program and legitimate interest assessment, these must be</td></tr>
</table>

	made available on demand to the OPC to ensure accountability. Section 8 continues the obligation under Canadian law to have a privacy officer.

Q5	***What is meant by "consent" as referenced in Bill 64 and Bill C-27?***
Bill 64	• Bill 64 provides that organizations have an obligation of transparency when dealing with PI, i.e. they must provide certain information in "clear and plain language" regardless of the means of collection used. This transparency obligation arises at the time of the collection (and subsequently upon request) or, in some cases, only upon request or in the context of the use of certain technologies (e.g. profiling). • Bill 64 updated the consent framework in Quebec – prior to Bill 64, consent had to be "manifest, free and enlightened," where it is now required to be "clear, free and informed." • Express consent is required where sensitive information is involved (see above for a definition of SI). • There are several new consent exceptions for using PI beyond the purposes for which it was originally collected, including: o Clearly, for the benefit of the person concerned; o Legitimate business purpose, i.e.: ▪ necessary for the prevention of fraud or the evaluation and improvement of protection and security measures; ▪ necessary for the supply or delivery of a product or the provision of a service requested by the person concerned; ▪ necessary for study or research purposes or for the production of statistics (subject to PI being de-identified).
Bill C-27	• Consent is still an essential requirement in many circumstances, but with C27, the bill introduces legitimate interest assessments to require businesses to balance the organization's interest against potential adverse effects on the individual (s. 18(3)). • Legitimate interests, however, are not available when the purpose is to influence an individual's decisions or behaviour.

Q6	***What is "profiling," as referenced in Bill 64 and Bill C-27?***
Bill 64	• Amendments in Bill 64 require organizations that collect personal information that would allow the person to be identified, located, or profiled to have these functions deactivated by default rather than activated by default. • Profiling is defined in Bill 64 to include any collection and use of personal information to assess certain characteristics of a natural person. This may have implications concerning Quebec and the international market.

Q7	*What obligations do organizations have when affected by a data breach, as defined in Bill 64 and Bill C-27?*
Bill 64	• There are breach reporting and notification obligations that have been introduced. • Security and protection measures, including technical, physical and administrative measures to protect personal information. Include incident registration requirements.
Bill C-27	• The CPPA continues with a data breach regime that is the same as in PIPEDA (which was amended in 2015 to include a data breach regime). • The threshold for reporting a breach is if there is a "real risk of significant harm."

Q8	*What obligations do organizations have when exporting data outside the jurisdiction where the data subject resides (i.e., Quebec, Canada)?*
Bill 64	• With respect to exporting data, Bill 64 adopts the "adequacy principle," wherein personal information should only be exported outside of Quebec to jurisdictions that have an equivalent level of protection for personal information as that found in Quebec. A privacy impact assessment ("PIA") must be conducted. This applies to personal information in the public and private sectors. If the PIA demonstrates that the personal information would not be adequately protected, then contractual arrangements must be taken to mitigate the risks. • For private enterprises, individuals must be informed of the possibility that their personal information could be communicated outside Quebec (through the privacy policy).
Bill C-27	• The CPPA doesn't change what we currently have in PIPEDA • Personal information can leave the country if: 1) there is notice and 2) there is a contract in place to adequately protect the information regardless of what jurisdiction it is moved to.

Q9	*What is a Privacy Impact Assessment; why are PIAs required?*
Bill 64	● Privacy impact assessments must be performed prior to the acquisition, development, and redesign of an information system, as required by Bill 64 as of Sept 2023. It must include an evaluation of the sensitivity of the information, the protection measures that apply to the information, and the relevant privacy framework.
Bill C-27	• It will be interesting to see if the draft CPPA might be amended by Parliament to include a PIA requirement.