May 31, 2019

PERSPECTIVE

Building a privacy-compliant autonomous vehicles business

Privacy law is a moving target and if you are building a business model around AV technology and expect to use even a fraction of the personal information generated by AVs, you will need to take developments in this area into account. Below, we highlight selected features of and recent developments in Canadian privacy law that you should be aware of and may want to factor into your business model.

The Canadian Privacy Law Landscape in General

In Canada, the Personal Information Protection and Electronic Documents Act ("PIPEDA") sets out ground rules for how private sector organizations and federal works, undertakings and businesses collect, use and disclose information about an identifiable individual ("personal information"), unless such activities are regulated by provincial legislation that has been declared substantially similar to PIPEDA. The provinces of British Columbia, Alberta and Québec have enacted general provincial personal information protection legislation that has been recognized as substantially similar to PIPEDA, and operates in place of PIPEDA in those provinces for intra-provincial matters. Where personal information crosses provincial or national borders, however, PIPEDA prevails.

Consequently, your business may be affected by one or more of these laws, depending on how and where you operate in Canada. Given that in the AV space, the primary generator of personal information is highly mobile, it is likely that a business operating in this sector will be subject to PIPEDA. Our comments in this article will focus on PIPEDA and the interpretations and guidance of the Office of the Privacy Commissioner of Canada ("OPC") that relate to PIPEDA.

Transborder Transfers of Personal Information

The OPC's position regarding the transfer of personal information between organizations located in different jurisdictions is changing.

In the past, the OPC has taken the position that a transfer of data to a third party that processes personal information on behalf of an organization (including but not limited to outsourcing arrangements, such as hosting data on a cloud provider) did not require the consent of concerned individuals.

On April 9, 2019, however, the OPC published a document entitled "Consultation on transborder dataflows" stating that the OPC is now of the view that transfers of personal information for mere processing activities between organizations located in different jurisdictions (*e.g.* between a Canadian company and its hosting service provider located in the US) would require the consent of concerned individuals.

This significant departure from the OPC's earlier position could have substantial consequences for any AV business that plans to use third party service providers for processing personal information.

However, following the Federal government's announcement of a new Digital Charter and of PIPEDA's upcoming reform that will address (among other things) cross-border data flows, the OPC has suspended the consultation in its current form while leaving the door open for its resumption in response to future developments. In the meantime, the OPC has not retreated from the new position articulated in the consultation document, nor has the OPC indicated that it will investigate new complaints in accordance with its earlier position.

Further comment on these matters will be provided in a separate bulletin in the near future. For now, companies in the AV space should monitor closely these developments.

Obtaining Meaningful Consent from Customers

In January 2019, the OPC's Guidelines for obtaining meaningful consent ("Guidelines") came into effect.

According to the Guidelines, consent should generally be express and can be implied only in "strictly limited circumstances". Organizations must generally obtain an individual's express consent if the information collected, used or disclosed is sensitive, or if the collection, use or disclosure of the information is outside the individual's reasonable expectations or creates a meaningful, residual risk of significant harm (including reputational harm) to the individual.

Recognizing that personal information or aggregations thereof collected by AVs may fall into one or more of those categories, you might reason that your organization can enumerate all of the potential uses and disclosures in a single policy upfront and take care of express consent obligations all at once. The Guidelines, however, criticize precisely this approach, discouraging "the use of lengthy, legalistic privacy policies that too often served to make control – and personal autonomy – make the individual control that should be enabled by consent nothing more than illusory". The OPC expects organizations to think about what they plan to do with personal information and the ways they plan to do it, and then carefully consider how to communicate that in a form that avoids information overload for "individuals with limited time and energy to devote to reviewing privacy information".

For additional information, please see our recent bulletin that considers the new Guidelines in further detail.

The proposed PIPEDA reform suggests introducing new basis to handle personal information beyond consent, including for "standard business activities". Further comment on this question will be provided in a separate bulletin in the near future.

Data Breach Reporting Requirements

As of November 2018, PIPEDA requires that organizations "in control" of personal information must keep records of all breaches of security safeguards involving personal information, report breaches involving that information to the OPC, and notify concerned individuals where it is reasonable to believe that there is a "real risk of significant harm".

The wide variety of systems and communication channels that AVs are expected to employ present a very large "attack surface". The more sophisticated the systems, the greater the potential for vulnerabilities that can be exploited, leading to greater risk of breaches of security safeguards involving personal information.

Moreover, breaches suffered by service providers, such as cloud computing or storage systems and third party data processors, must also be accounted for. Where an organization has transferred personal information to a third party for processing and a breach occurs while the information is with the processor, under PIPEDA, the obligation to report remains with the principal organization – the one "in control" of the personal information.

For further discussion, please see our recent commentary on data breach reporting.

Upcoming IoT guidance from the OPC

The OPC has announced that it will release shortly new guidance regarding Internet of Things (IoT) for product manufacturers. Such guidance will be relevant for AV businesses. Companies in the AV space should closely monitor these developments.

Concluding Remarks

Privacy law is a moving target. Given the constantly changing dynamic between information use, the economy and society, we expect legal frameworks governing privacy and data protection will continue to evolve. This creates the potential to break business models that fail to account for these developments. As the privacy landscape changes, organizations may find that being proactive about privacy and data protection can help ensure a smooth path forward.

By: Elisa Henry, Max Jarvie

Services: Cybersecurity, Privacy & Data Protection, Autonomous Vehicles

---

Table of contents

2023 Series

- Autonomous vehicle laws in Canada: Provincial & territorial regulatory review - January

2022 Series

Autonomous vehicles: Key 2022 industry hotspots – April

Autonomous vehicle laws in the States: Congress offers hope for national regulatory framework – June

Autonomous vehicles: cross jurisdictional regulatory perspectives update – October

2021 Series

Autonomous vehicles: Moving forward in 2021 – January

Full steam ahead: Recent developments in maritime autonomous technology – February

Next-gen spotlight: 5G, autonomous vehicles and connected devices – March

Raising financing during turbulent times: Debt capital options for tech companies – April

Construction and autonomous vehicles: Considerations for increased adoption – May

Autonomy on the roads: Intelligent Transportation Systems – June

Autonomous vehicles in mining operations: Key legal considerations – July

Autonomous technology in Calgary: Reducing emergency vehicle travel times – August

Autonomous vehicles: Cross jurisdictional regulatory perspectives –September

Transport Canada: 2021 Guidelines for Testing Automated Driving Systems in Canada – October

Autonomous vehicles: Canada's readiness for the future – November

Autonomous vehicle laws in Canada: Provincial & territorial regulatory landscape – December

2020 Series

Driving change: The year ahead in autonomous vehicles – January

Mobility-as-a-service & smart infrastructure: A new risk paradigm – February

The future of farming: Autonomous agriculture – March

Autonomous transportation in the time of COVID-19 – April

Driverless vehicles: Two years of autonomy on Québec roads – May

A review of Canada's vehicle cybersecurity guidance – June

Highlights of the connected and autonomous vehicles report by ICTC and CAVCOE – July

Raising financing during turbulent times: The takeaways – August

Raising financing during turbulent times: Exploring for capital in the public markets – September

Advanced driving assistance systems: Three issues impacting litigation and safe adoption – October

Autonomous vehicles and big data: Managing the personal information deluge – November

Payments on wheels: Self-driving vehicles and the future of financial services – December

2019 Series

The Legal Crystal Ball: Autonomous Vehicles Development to Watch For in 2019 – January

Autonomous Vehicles and Export Controls – February

The State of Insurance and Autonomous Vehicles in Ontario – March

Collective Bargaining and the Implementation of Autonomous Vehicles Technologies – April

Building a Privacy-Compliant Autonomous Vehicles Business – May

The State of Autonomous Vehicles in Alberta – June

Unfamiliar Waters: Navigating Autonomous Vessels' Potential and Perils – July

The Lay of the Land: Obtaining a License for Testing Autonomous Vehicles in Ontario – August

The State of Autonomous Vehicles in Saskatchewan – September

Lingua Vehiculum: The Competition for Connected Car Communication – October

Autonomous Vehicles and Equipment in Construction – November

The Future of Mobility: The 2020 Autonomous Vehicles Readiness Matrix Legal Summit – December

2018 Series

Current Industry Developments – February

Managing Cybersecurity Risks – March

Québec Regulation Update – April

The Connected City – May

Are Patent Wars Coming for AVs? – June

Automated Vehicles May Revolutionize Mobility but Perhaps not Auto Insurance – July

Cleared for Take-off: Autonomous Technology and Aviation Litigation – August

The Ultimate Mobility Synergy: Autonomous Vehicles and Electric Vehicles – September

Automotive and Insurance Industries Consider Hot Issues Faced by the Autonomous Vehicles Sector – October

Insuring Automated Vehicles: The Insurance Bureau of Canada Recommends "Single Insurance Policy" – November

Autonomous and Connected Vehicles – "Ideal" for a Class Action? – December