Building a privacy-compliant autonomous vehicles business

May 31, 2019

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

Expertise

Cybersecurity, Privacy & Data Protection, Autonomous Vehicles

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.