November 30, 2020

We have commented before in *The Sensor* on the general privacy and data protection implications for the connected and autonomous vehicles (CAVs) ecosystem. In this issue, we return to consider those implications in relation to recent developments in the world of CAV big data.

The Automotive Edge Computing Consortium (AECC) researches how edge network architectures could help CAVs process data effectively within the timeframes needed to support current and next generation CAV technologies and enterprise applications. These technologies and applications include High Definition Mapping, Intelligent Driving, Mobility Services and Finance and Insurance services.[1]

In its most recent publications and presentations, the AECC concluded that earlier studies of the data required for CAVs in relation to these services greatly underestimated the volume of data needed. When the technologies mentioned above are taken into account, current estimates suggest that each vehicle could be generating up to 100 GB of data per month. Across an estimated 100 million CAVs in use worldwide by 2025, that could mean as much as 10 exabytes of data per month.[2]

In our previous article, we referred to the amount of data generated by CAVs as a torrent. These recent studies on data volumes reveal that the metaphor of a tsunami or deluge is likely more appropriate. As a significant quantity of this information will be personal information, the volume of data and the complexity of the multitier information ecosystems needed to support its processing will create challenges for privacy and data protection.

Privacy challenge one: Managing contractual relationships

Edge computing provides an intelligent solution to the basic problem of managing and timely processing large quantities of data. However, with so much information circulating through multitier network architectures, organizations providing services that use them need to be aware of where the data is flowing, and who ultimately has access. Important considerations include such questions as:

- What are the relationships between the entities processing data, from the edge to the centre? For example, is there a clear hierarchical service provider relationship between them, or are they partners or joint ventures? Do they have certain independent rights around the use of the data flowing through these systems?
- What is the legal relationship between my organization and the entities involved in the CAV ecosystem?
- If my organization is contractually bound to only one entity at the edge, how do all the relevant legal obligations around data security, obtaining consent and liability flow up and down through the contractual chain? For example, how are auditing rights and access to information requests managed down the contractual chain?

If my organization is contractually bound to only one entity at the edge, how do all the relevant legal obligations around data security, obtaining consent and liability flow up and down through the contractual chain? For example, how are auditing rights and access to information requests managed down the contractual chain?

Understanding these relationships will be crucial, both for properly drafting the contracts between an organization offering CAVs' services and the entities operating the information processing systems that will govern the use of personal information, and for understanding the organization's own responsibilities with respect to such matters as obtaining consent from individuals whose personal information is used.

Privacy challenge two: Meaningful consent

Canadian private sector privacy laws are consent-based: subject to certain exceptions, organizations must obtain consent for the collection, use and disclosure of personal information, and regulators expect them to meet the challenge of obtaining *meaningful* consent.[3]

Privacy policies are typically used as a way to consolidate information about privacy and data handling practices, but regulators increasingly expect organizations to find ways to communicate salient information in a form that can be easily understood, particularly by those who do not have the time to read and digest lengthy privacy policies.

Regulators now expect organizations to be, among other things, creative in their approaches, for example by using just-in-time notices, interactive tools or infographics. Organizations are also expected to allow individuals to control the level of detail they get and when and emphasize key elements, such as what personal information is being collected; with which parties personal information is being shared; for what purposes personal information is collected, used or disclosed; and residual risk of harm and other consequences.[4]

Satisfying these obligations is a significant challenge, and all the more so when one considers complex information ecosystems such as those examined by AECC. We can hope that, in the future, privacy law reforms in Canada will introduce legal basis other than consent for the collection, use and disclosure of personal information, as the EU has done.[5] In the meantime, CAVs organizations in Canada should pay attention to the obligation to provide control over the level of detail provided to individuals, for example by offering layers of elucidation that span the interpretability/explainability divide.[6]

Organizations that need to provide explanations of how information moves within a system in order to explain how it is collected, used and disclosed should consider investing time in the layered approach. For example, organizations can provide top-level summaries that provide just enough information for individuals in a hurry to get a sense that there are many participants and directions in which information is flowing; a second level that goes into some detail, perhaps with a summary black-box diagram; and a third layer, that provides a closer view and more detailed infographics.

Privacy challenge three: Privacy by design

Between the requirements to obtain meaningful consent and the challenges of ensuring contractual protections, organizations might feel that the complexities of the edge computing model for CAVs services creates privacy law risks that are difficult to quantify or control. For this reason, organizations may want to consider Privacy by Design (PbD).[7] While always good practice, adopting a PbD approach might be particularly useful in the CAVs multitier information processing contexts.

PbD means calls for privacy be taken into account throughout the engineering process. In the CAV edge computing context, this could translate into determining what the organization really needs to collect, use or disclose, in order to provide the service; engineering the system to strip out as much personal information as possible, as early as possible, in order to reduce the attack surface of the system; and using advanced techniques – such as homomorphic encryption,[8] private set intersection,[9] and others – to minimize exposure of personal information as it makes its way from CAVs to edge to centre.

The principles of PbD are sometimes criticized as vague and not easily translated into engineering practice.[10] In fairness to the champions of PbD, however, it should be mentioned that PbD is a set of principles, not specific practices. By having engineers, product owners and other stakeholders absorb those principles, organizations can put themselves in a position to fashion PbD solutions specific to a particular service, product, or line of business. Moreover, while the merits of specific PbD principles can be debated, as a whole they represent a set of regulative ideals that can assist organizations in reducing the risk of handling and transacting personal information.

Final word

Organizations confronting the CAVs data deluge will need to arm themselves with a variety of solutions. Just as edge computing can help meet the processing challenges, consideration of the matters discussed here can help organizations to meet privacy law challenges.

---

[1] See *e.g.*, Automotive Edge Computing Consortium, "AECC Technical Report v2.0: Driving Data to the Edge: The Challenge of Data Traffic Distribution," July 2020; Automotive Edge Computing Consortium, "Operational Behavior of a High Definition Map Application (White Paper)," May 26, 2020; Prashant Tiwari, "Managing the Connected Car Data Tsunami" presented at *Edge Computing World* 2020, Oct. 14, 2020; Ken-ichi Murata, "Edge Computing for the Connected & Autonomous Car," presented at *Edge Computing World* 2020, Oct. 14, 2020.

[2] Tiwari, Prashant, "Managing the Connected Car Data Tsunami," presented at *Edge Computing World* 2020, Oct. 14, 2020. To better appreciate the scale, consider: 1000 terabytes = 1 petabyte; 1000 petabytes = 1 exabyte. While accurate estimates are hard to come by, Google is thought to process approximately 200 petabytes per day.

[3] See *e.g.* the Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent", May 18, 2020.

[4] *Ibid*.

[5] The European Union's *General Data Protection Regulation* (GDPR) provides six legal bases: consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and public interest: see article 6, GDPR.

[6] Often raised in the context of AI, but applicable generally. Many systems that we interact with every day are interpretable to us, but not necessarily explainable, such as mobile phones, cars and elevators. For most people, such systems are black boxes. Through experience, individuals will come to associate a variety of inputs with outputs, reactions or responses, and can also make successful predictions about how one of these systems would react to a certain input. Most of us typically rely on interpretability: we skip the (many) details that we would not understand anyway, or have no interest in taking the time to learn. See e.g. Leilani H. Gilpin et al., "Explaining Explanations: An Overview of Interpretability of Machine Learning," Feb. 3, 2019.

[7] See *e.g.*, Ann Cavoukian, "Privacy by design: The 7 foundational principles," Information and Privacy Commissioner of Ontario, 2009.

[8] Bernard Marr, "What Is Homomorphic Encryption? And Why Is It So Transformative?" Forbes, November 2019.

[9] Hao Chen, Kim Laine and Peter Rindal, "Fast Private Set Intersection from Homomorphic Encryption," CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, October 2017.

[10] Jeroen van Rest, "Designing Privacy-by-Design," *Designing Privacy by Design: Lecture Notes in Computer Science* (2014) pp. 55–72; Seda Gurses, Carmela Troncoso, and Claudia Diaz, "Engineering Privacy by Design."

By: Max Jarvie

Services: Disputes, Insurance Claim Defence, Transportation, Automotive, Autonomous Vehicles

---

Key Contacts

Robert L. Love
PARTNER

Toronto

RLove@blg.com

416.367.6132

Luke Dineley
PARTNER

Vancouver

LDineley@blg.com

604.640.4219

Josiane Brault
PARTNER

Montréal

JBrault@blg.com

514.954.2557

Edona C. Vila
PARTNER

Toronto

EVila@blg.com

416.367.6554

Table of contents

2024 Series

- Ontario's newly proposed pilot program for automated commercial vehicle testing - November

2023 Series

- Autonomous vehicle laws in Canada: Provincial & territorial regulatory review - January
- Driving into the future: U.K. announces regulatory scheme for the use of automated vehicles - December

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