June 30, 2020

PERSPECTIVE

A review of Canada's vehicle cybersecurity guidance

Connected and automated vehicles (CAVs) present opportunities and risks for Canada's transportation industry. CAVs have a number of valuable features that could enhance safety, efficiency and accessibility of roads.[1] However, due to their sophisticated systems and connectivity to external communication devices and infrastructure, CAVs present novel cybersecurity risks that can threaten the safety and privacy of passengers.

It is against this backdrop that in March 2020, Transport Canada published *Canada's Vehicle Cyber Security Guidance* (Guidance), which provides a risk-based approach for organizations involved in the automotive industry to assist with identifying, managing and detecting cybersecurity risks throughout a vehicle's life cycle.

Although the Guidance focuses on cybersecurity rather than privacy, the overlapping considerations enrich the conversation concerning the reform of Canada's privacy laws initiated by the publication of the federal government's 2019 *Digital Charter*. In particular, the Guidance's endorsement of the development of an industry code of practice speaks directly to an important aspect of that discussion. While the CAV ecosystem could benefit from the articulation of industry norms and best practices, how these will fit into a future regulatory scheme remains to be seen.

Below, we review the key aspects of the approach taken and conclude with some comments on its interaction with privacy laws in the context of anticipated legal reforms.

The four principles

The Guidance outlines four technology-neutral and non-prescriptive principles designed to enhance the cybersecurity of CAVs by identifying, monitoring and responding to related risks. Those principles are:

- Identify and manage cybersecurity risks;
- Protect the vehicle ecosystem by implementing adequate safeguards;
- Detect, monitor and respond to cybersecurity events; and
- Recover from cybersecurity events safely and quickly.

The Guidance's risk-based approach is influenced heavily by existing guidance documents, including those by the U.S. National Institute of Standards and Technology and the Automotive Information Sharing and Analysis Centre.[2] Although the Guidance offers a uniquely Canadian perspective to the issue of cybersecurity in the automotive industry, it generally follows a broader global trend towards non-prescriptive cybersecurity principles espoused by other jurisdictions.

As mentioned, although the Guidance concentrates on cybersecurity rather than privacy and data protection, it is interesting to note that the principles expressed in the Guidance parallel in some respects those found under the federal *Personal Information Protection and Electronic Documents Act*[3] (PIPEDA). Indeed, mention of PIPEDA and the institutions that administer and enforce it surfaces at several points, and, as discussed further below, notions of accountability, transparency and "appropriate" (*i.e.* commensurate) security safeguards are at the forefront of the Guidance's risk-based approach.

Identiying and managing cybersecurity risks

- Cybersecurity governance: Organizations are advised to develop formal, documented governance frameworks that clearly identify roles and responsibilities within their organizations related to managing cybersecurity risks. In order to be effective, senior executives should champion these frameworks and they should be reviewed, assessed and improved regularly.
- Risk management frameworks: A risk-based approach also requires organizations to adopt a documented risk management strategy that addresses risks to ensure the safety of critical systems and personal information. In addition, organizations are encouraged to implement asset management practices to inventory vehicle and equipment components, including data assets, and assess their value for the purposes of implementing appropriate risk-based security controls.
- Supply chain security: Given CAVs' "heavily-tiered and increasingly non-traditional supply chain,"[4] responsibility for protecting cybersecurity should be shared by all actors involved in this supply chain. Thus, the Guidance suggests imposing contractual measures on service providers, vendors and sub-contractors to guarantee that they respect specific security requirements. According to the Guidance, these measures need auditing regularly, according to a predetermined schedule.

Protecting the vehicle ecosystem

- Layered cyber defences: Avoiding an overly formalistic set of technical solutions, the Guidance focuses on a "defence-in-depth" approach that layers cybersecurity solutions and sets out a number of overlapping "security goals," including appropriate security controls, data security using adapted cryptographic techniques, secure internal and external communications, identity management and access control, secure software development, and secure updates.
- Privacy protection and information protection procedures: The Guidance acknowledges that Canadian privacy laws – including PIPEDA and substantially similar provincial laws – are difficult to apply to particular industries that present novel privacy challenges due to their technologically neutral language. This is particularly true of CAVs, as there are a number of industry stakeholders that may share varying degrees of responsibility for complying with Canadian privacy laws. In this context, it is not readily clear how certain privacy principles, such as consent, data minimization and purpose limitation, should be respected, especially considering the "unprecedented amounts of data on passenger movements and mobility habits" that could be collected by these vehicles.[5] This large volume of data may be used in a number of ways that are neither obvious nor apparent to the average consumer, which raises concerns about over-collection and misuse of personal information.[6]

Despite these issues, the Guidance offers scant recommendations in terms of applying Canadian privacy law principles with respect to CAVs, preferring instead to focus on the future development of an industry-specific code of best practices. Indeed, according to the Guidance, the Canadian government has committed to working with the Office of the Privacy Commissioner of Canada and other stakeholders to develop an industry-specific code of best practices for privacy protection.[7] This idea also finds support in earlier statements made by Innovation, Science and Economic Development Canada (ISED) regarding PIPEDA's reform, in which ISED noted that it is contemplating creating a formal role for codes, standards and certification under PIPEDA.

- Training and Awareness Programs: Organizations should implement adequate training and awareness programs to inform relevant stakeholders, including employees, users and owners, about potential cybersecurity risks.

Detecting, monitoring and responding to cybersecurity events

- Event detection, monitoring and analysis and vulnerability management plan: Organizations should have measures in place to rapidly detect, monitor and analyze cybersecurity threats and vulnerabilities in their operating environment. In turn, this information should be shared internally and externally to maximize its impact.
- Security audits: The Guidance recommends that security best practices and controls be verified through regular, objective, independent and documented assessments and periodic audits, including penetration testing of systems, networks and applications.
- Incident management and response: Organizations should implement a robust incident management plan to respond to cybersecurity incidents in a methodical, co-ordinated way. Response processes, roles and responsibilities, incident containment measures and escalation procedures are some of the key areas that need clear identifying and defining in the plan.

Recovering safely and quickly from cybersecurity events

- Incident recovery: The Guidance outlines a number of steps organizations should take to recover from a cybersecurity incident. These include conducting a post-incident analysis and system diagnostics in order to identify associated vulnerabilities, take remedial measures and document lessons learned.
- Partnership building and information sharing: Throughout the Guidance, emphasis is placed on collaboration between the various stakeholders involved in the automotive industry, including manufacturers, suppliers, service providers and government bodies.
- Cybersecurity as a process of continuous improvement: The Guidance generally recognizes that eliminating all cybersecurity risks with respect to CAVs is not feasible or realistic. As such, the Guidance focuses on the need to learn through periodic reviews and audits of security systems, by documenting lessons learned and applying those lessons in the future.

Conclusion

The Guidance represents an important, albeit cautious, step towards developing a comprehensive cybersecurity regulatory framework for CAVs, but we can expect future legislative developments to provide greater clarity, especially related to PIPEDA's anticipated reform. It remains to be seen whether this is via regulatory requirements or a best practices code. This will depend on whether the legal reforms to Canadian privacy laws maintain a technology-neutral approach. Even if those reforms do find a place for codes, however, it would be premature to expect this to manifest as a fully-fledged self-regulatory regime for cybersecurity.

In *Strengthening Privacy for the Digital Age*, ISED noted that integrating codes and standards within Canada's federal privacy statute may serve to enhance transparency and certainty for individuals, promote interoperability between international privacy law frameworks and relieve regulators of compliance work. In that same document, however, ISED highlights concerns over enforceability of these self-regulatory regimes, noting that without appropriate oversight, they can be at best meaningless and at worst deceptive.

In this respect, ISED suggests proactive oversight by the Office of the Privacy Commissioner of Canada.[8] Given the quasi-constitutional character of privacy laws, we would not expect ISED to delegate regulatory authority in this domain to a CAV self-regulatory body in any robust sense. To the extent that Transport Canada would support a self-regulatory body for CAVs that included cybersecurity, these considerations would have an impact on the scope of such a body's authority and oversight powers.

It bears mentioning that there is also a certain tension between the risk-based framework the Guidance proposes and the broader trend towards a rights-based approach to privacy law.[9] While not in formal opposition, rights-based approaches tend to rely on analyses of necessity and proportionality rather than risk, and consequently tend to be better adapted to dealing with potential infringements of individual rights in the face of emerging technological developments and other new contexts.[10] To the extent that Canada adopts a rights-based framework in the course of reforming its privacy laws, formal regulatory endorsement of a risk-based approach seems unlikely.

This article was co-written by Andy Nagy, Articling Student.

---

[1] Canadian Council of Motor Transport Administrators, *Canadian Jurisdictional Guidelines for the Safe Testing and Deployment of Highly Automated Vehicles*, June 2018, page 13.

[2] Transport Canada, *Canada's Vehicle Cyber Security Guidance*, March 2020, page 12.

[3] S.C. 2000, c. 5.

[4] Transport Canada, *Canada's Vehicle Cyber Security Guidance*, March 2020, page 9.

[5] Transport Canada, *Safety Assessment for Automated Driving Systems in Canada*, January 2019, page 19.

[6] It is interesting to note, for instance, that according to the Canadian Council of Motor Transport Administrators, authorities may eventually seek to use this data for law enforcement purposes. See Canadian Council of Motor Transport Administrators, *Canadian Jurisdictional Guidelines for the Safe Testing and Deployment of Highly Automated Vehicles*, June 2018, pages 55-61.

[7] Transport Canada, *Canada's Vehicle Cyber Security Guidance*, March 2020, page 17.

[8] The Office of the Privacy Commissioner of Canada has also raised similar concerns regarding self-regulation. See Office of the Privacy Commissioner of Canada, *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*, 2019.

[9] For instance, see the Office of the Privacy Commissioner of Canada, *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*, 2019.

[10] As stated by the Office of the Privacy Commissioner of Canada, technical protections are "often ineffective as they are regularly overtaken by

developments in technology." Office of the Privacy Commissioner of Canada, *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*, 2019.

By: Max Jarvie, Andy Nagy

Services: Transportation, Autonomous Vehicles, Automotive, Online Retail & E-commerce

Key Contact

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

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