

December 14, 2018

PERSPECTIVE

Autonomous and Connected Vehicles — “Ideal” for a Class Action?

Why Autonomous Vehicles?

The technical capabilities of autonomous vehicles continue to advance and impress. Features such as automated self-parking are now blasé, making way for technology that enables vehicles without steering wheels or pedals to be manufactured in 2019.¹ During operation, autonomous and connected vehicles generate and can record a significant amount of information including driving input, speed, and direction. Vehicles currently on the road may offer connected services for communications and driver aids (e.g. camera rear-view mirror, emergency braking, and reverse auto braking, etc.).

While impressive, these technologies (and the data creation that comes with them) risk system exploitation, data breach and product-wide issues. Researchers have already demonstrated the ability to penetrate connected systems² and the risks of privacy breaches are all too well known. As increasing amounts of information are recorded and stored by autonomous vehicles or uploaded to connected servers, data from autonomous and connected vehicles will become more valuable to third-party hackers. Software or programming issues that could render an autonomous feature inadequate or unsafe would likely apply to all vehicles across a product range rather than individual vehicles.

This article considers two likely avenues for future autonomous vehicle class action litigation - privacy and product liability.

Privacy Class Actions

In the event that private data is accessed or disclosed as a result of a cybersecurity vulnerability, a class action provides one option for affected consumers. Privacy class actions are nothing new to Canada and have resulted in significant monetary settlements. While individual payments to class members are often nominal (from around \$2,500³ to \$5,000⁴ each), large class sizes have the potential to result in a high total damages award in addition to other expenses such as counsel fees and settlement administration. As an example of such exposure, in a recent case relating to a breach of personal and financial information, a defendant paid out approximately \$1.25 million.⁵

While there have yet to be any class actions commenced in Canada for issues relating to connected and autonomous vehicles, recent litigation in the United States has considered claims relating to cybersecurity vulnerabilities in connected vehicles with varying results.

In *Cahen, et al. v. Toyota Motor Corp.*, et al.⁶, plaintiffs alleged that certain Toyota vehicles had insufficient security measures and sought damages on the basis that the vehicles could be vulnerable to hacking despite the fact that no hacking had actually occurred. The district court dismissed the case, finding that the plaintiffs had not sufficiently alleged an injury which was specifically linked to the risk of hacking itself. This decision was upheld on appeal.⁷

In contrast, plaintiffs in a putative class action brought against Fiat Chrysler, *Flynn et al. v. FCA US LLC et al.*⁸, were partially successful in being permitted to proceed with claims relating to the risk of hacking. The action was commenced after software was updated to protect against potential hacking vulnerabilities. Although the Court dismissed claims for possible future hacking events, it permitted the plaintiffs to proceed with claims that their vehicles depreciated in value due to risk of hacking. Fiat Chrysler has requested leave to seek an interlocutory appeal, stating that “all connected products are potentially ‘vulnerable’ to hacking” and that an action alleging that a product could be vulnerable was not sufficient for certification.⁹

In Canada, manufacturers will want to continue to design their autonomous systems with sufficient protection to guard against the potential for privacy breaches in order to avoid a class action. Given the experience in the U.S., class actions brought to address potential future problems that have yet to materialize will likely be met with challenge.

Product Liability Class Actions

It is often suggested that product liability cases are “well-suited” or “ideal candidates” for class action treatment, as proof of a defect or product issue can be extrapolated to all of those who have purchased the same product.¹⁰ In Canada, a number of automotive claims have been deemed appropriate to be certified as a class action.¹¹

A class action may not, however, be appropriate in cases where a common question is not easily posed. This may occur in circumstances where manufacturing techniques change over time, there are multiple parties involved in delivering the finished product to a consumer or there is a change in the appropriate standard of care.¹² Given the pace of technological improvement and the complexity of the technical matters likely to be in issue, the importance of submitting evidence from an adequate expert to give some evidentiary basis for the claim cannot be ignored.¹³

“Commonality” will likely be a fertile battle ground for litigation relating to autonomous vehicles. In a product liability action, arguments usually focus upon the similarities (or differences) between the products which are alleged to have been defective.

As an illustrative example, three similar putative class actions considered product liability claims in relation to medical devices, but each arrived at separate results on certification.¹⁴ Two actions which alleged issues with a wide range of similar, but varied, products were deemed inappropriate for certification – the defendant’s conduct differed among the products and no common defect across all products was identified.¹⁵ An action that focused on one “single undifferentiated product group” was deemed appropriate for certification as the parties did not draw distinctions between the devices.

Looking Forward

While autonomous or connected vehicles have yet to be the subject of a class action in Canada, the plaintiff’s bar will be certain to raise issues which will test the boundaries of class proceedings.

Manufacturers and other parties responsible for the collection, use and storage of data gleaned from these productions should remain aware of the legal risks associated with maintaining data. Canada has already gained experience with class actions arising from privacy breaches, but there is an open question as to what type of loss will be sufficient to give rise to a certifiable class action.

Manufacturers and distributors of autonomous and connected vehicles remain exposed to the possibility of a product liability class action, but it is not yet clear whether the issues regarding these vehicles will be simple or narrow enough to be answered in common across a class. Largely, this will depend on the specific defect being alleged and the degree to which that defect is manifested across the series of products tied to a prospective class definition. It remains to be seen how these products will be dealt with on a motion for certification.

For further information on the process and steps of a class action, please visit the class actions section of [*BLG's Product Liability Handbook*](#).

¹ Alex Davies, [*GM Will Launch Robocars Without Steering Wheels Next Year*](#) (January 2018), WIRED.

² Chris Valasek and Charlie Miller, [*Remote Exploitation of an Unaltered Passenger Vehicle*](#), IOActive ; Andy Greenberg, [*Hackers Remotely Kill a Jeep on the Highway – With Me In It*](#), WIRED.

³ *Maksimovic v. Sony of Canada Ltd.*, 2013 CanLII 41305 (Ont Sup Ct J).

⁴ *Lozanski v. The Home Depot, Inc.*, 2016 ONSC 5447.

⁵ *Drew v. Walmart Canada Inc.*, 2017 ONSC 3308.

⁶ Heather Sussman, Doug Meal, and David Cohen, Recent Decisions Highlight Product Cybersecurity Issues re: *Cahen, et al v Toyota Motor Corp.*, et al – US District Court Northern District of California.

⁷ *Helene Cahen, et al. v. Toyota Motor Corp.*, et al., No. 16-15496, 9th Cir., 2017 U.S. App. LEXIS 26261.

⁸ *Flynn, et al. v. FCA US LLC, et al.*, Case No. 3:15-cv-00855.

⁹ Linda Chiem, *Fiat Chrysler Asks Justices to Review Car-Hacking Cert. Order* (October 2018), online: Law 360.

¹⁰ *Williams v Canon Canada Inc.*, 2011 ONSC 6571 at para 125 [Williams]; *Schick v Boehringer Ingelheim (Canada) Ltd.*, 2011 ONSC 1942 at para 74.

¹¹ *Thorpe v Honda Canada Inc.*, 2011 SKQB 72 [Thorpe]; *Reid v Ford Motor Company*, 2003 BCSC 1632; *Kalra v Mercedes Benz*, 2017 ONSC 3795.

¹² *Ernewein v General Motors of Canada Ltd.*, 2005 BCCA 540 at para 33.

¹³ *Williams, supra*; *Thorpe, supra*.

¹⁴ *O'Brien v Bard*, 2015 ONSC 2470 [O'Brien]; *Vester v Boston Scientific Ltd.*, 2015 ONSC 7950 [Vester]; *Dine v Biomet*, 2015 ONSC 7050 [Dine].

¹⁵ *O'Brien, supra*; *Vester, supra*.


By: [John Hunter](#), [Glenn Zakalib](#)


Services: [Disputes](#), [Class Actions](#), [Cybersecurity](#), [Privacy & Data Protection](#), [Privacy Regulators' Investigations](#), [Privacy & Security Breaches](#), [Autonomous Vehicles](#)

Key Contacts

John Hunter
Partner

 Toronto

 JHunter@blg.com

 [416.367.6339](tel:416.367.6339)

Glenn Zakaib
Senior Counsel

 Toronto

 GZakaib@blg.com


 [416.367.6664](tel:416.367.6664)

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

