Managing Cybersecurity Risks of Connected and Autonomous Vehicles

March 23, 2018

The risk of cyber breaches is not only a concern associated with autonomous vehicles: technology, already available in connected vehicles, carries the same risks. This technology allows for various levels of connectivity ranging from systems used for communications and entertainment (*e.g.* Ford's SYNC, GM's On Star, Toyota's Entune, Cadillac's CUE, and Chrysler's UConnect) to driving assistance (*e.g*. camera rear-view mirror, emergency braking, and reverse auto braking, etc.).

Several studies have demonstrated the ability to remotely hack into connected vehicles. The first public cyber-attack on a connected vehicle occurred in 2015 – as an experiment. The code used by the researchers allowed them to send commands through the vehicle's entertainment system to its dashboard functions, steering, brakes, and transmissions – all from a laptop in a remote location. The experiment progressed to the point where the researchers were able to cut the transmission of the vehicle, forcing the vehicle to stop in the middle of an interstate highway.[1] Outside of controlled research, there are a multitude of cybersecurity threats involving personal financial data and identity theft (targeting online automotive apps and services that contain banking or credit records); freight and goods theft (targeting systems in connected trucks that cause cargo to be left unattended); and ransomware (disabling a function in the vehicle and demanding payment in exchange for restoring the function).

Autonomous or self-driving vehicles, unlike connected vehicles, will require a higher level of automation and connectivity with other sources, including the infrastructure around the vehicle. Automation increases data specification and produces a higher volume of data. The stakes of cyber breaches in autonomous vehicles will be more significant as the data will become even more valuable to third-party hackers. The ramifications of such cyber breaches on business are significant. Absent specific cybersecurity regulation for connected and autonomous vehicles in Canada, recent litigation involving cyber-attacks is helpful to illustrate the potential legal and business risks associated with such intrusions in the automotive industry.

The past five years have seen a significant rise in class action lawsuits in Canada stemming from cyber breaches, many of which have been certified to proceed, and some of which have resulted in court-approved settlements. In most of these cases, the remedies available for each class member are nominal (ranging from $2,500 to $5,000 per claimant), however, the total exposure to damages and counsel fees can be

significant depending on the size of the class. For example, the 2017 class action settlement approval in Drew v Walmart Canada Inc.,[2] had an assessed exposure of $1.25 million, including up to $5,000 reimbursement for any class member, one-year-long credit monitoring, and $250,000 in counsel fees. In that case, the data breach in Walmart's online photo printing software resulted in the access of personal and financial customer information. In a related cyber-attack class action settlement[3] affecting 3.5 million Sony account holders, Sony was to reimburse each class member up to $2,500. Counsel fees under the settlement were approved at $265,000.

While there has yet to be any litigation involving connected vehicles in Canada, it is worth reviewing two such class actions commenced in Illinois and California. These cases have seen vastly different results. The California[4] decision relates to claims for damages on the basis of potential hacking events that could take place due to allegedly low-level-security measures in certain Toyota vehicles. That case was dismissed in its entirety by the Court because the plaintiffs failed to sufficiently allege injuries due to the risk of hacking, overpaying for their vehicle, and invasion of their privacy. In contrast, a lawsuit against Fiat Chrysler filed in Illinois[5] has enjoyed a different life cycle. The lawsuit stems from a 2015 recall where Fiat Chrysler vehicles equipped with Uconnect 8.4A or Uconnect 8.4AN systems were updated to fix any potential hacking vulnerabilities. Initially, the Court dismissed the claims for possible future hacking events. However, the Court has since allowed the plaintiffs to proceed with claims that their vehicles depreciated in value due to risk of hacking. In response, Fiat Chrysler has argued that there is no liability for theoretical hacking events and no evidence that the vehicles have depreciated in value. It will be interesting to monitor what the Court's ruling will be in this case.

Cyber breaches also present significant regulatory risks. Such regulatory proceedings present additional defence costs, reputational and business losses, and potential regulatory penalties. Under recently proposed regulations to the Personal Information Protection and Electronic Documents Act (PIPEDA), organizations are to notify affected individuals and report to the Office of the Privacy Commissioner of Canada "as soon as feasible" following a data breach event. The threshold of such reporting is based on the "real risk of significant harm" to any individual whose personal information may have been breached. Failure to notify the federal regulator carries a fine of up to $100,000, along with a private right of action by individuals affected from the breach.

The 2016 class action settlement approval case involving the criminal hacking of Home Depot's card payment system illustrates the benefits of providing timely notification to the appropriate privacy regulators[6]. In that case, Home Depot proceeded to notify the federal privacy regulator and four provincial privacy regulators. None of the regulators proceeded with an investigation following notification of the breach. Instead each regulator closed its respective file. This demonstrates the importance of risk mitigation strategies such as a proactive incident breach response to reduce risk of prosecution by relevant privacy regulators. However, as demonstrated by the 2016 joint investigation report on the Ashley Madison data breach conducted by the federal privacy regulator and its Australian counterpart, regulators will not hesitate to proceed with an investigation. In that case, the regulators found numerous violations of privacy laws[7].

Although we are currently operating in somewhat of a regulatory vacuum, some regulatory oversight may be on the horizon for the auto sector. The Office of the Privacy Commissioner announced early in 2017 that it would be funding an arms-length project

to develop a code of practice for connected and autonomous vehicles. The Privacy Commissioner expressed agreement with the "privacy by design"[8] approach whereby the sector takes into consideration security and privacy from the outset of the innovation process[9]. While this approach may assist in inoculating the industry against cybersecurity breaches related to new technologies in the future, organizations are currently left to mitigate against these breaches related to current connected technologies.

The takeaway for the automotive sector is that while Canada has yet to roll out specific cybersecurity statutory or regulatory requirements with respect to connected and autonomous vehicles, class actions and regulatory prosecution by the privacy regulators present significant legal and business risks for stakeholders. The risk is present in the technology available today and may become even more significant with emerging autonomous vehicle technologies.

[1] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It", (21 July 2015). See also the White Paper by Chris Valasek and Charlie Miller, "Remote Exploitation of an Unaltered Passenger Vehicle" (2015).

[2] *Drew v Walmart Canada Inc.* 2017 ONSC 3308 (Ontario).

[3] *Maksimovic v Sony of Canada Ltd.* 2013 CanLII 41305 (Ontario).

[4] 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.

[5] Christopher Crosby, Jeep Drivers Fight For Class Cert. in Hacking Suit re: *Flynn et al v FCA US LLC, et al*. US District Court Southern District of Illinois.

[6] *Lozanski v Home Depot* 2016 ONSC 5447 (Ontario) at para 7.

[7] PIPEDA Report Findings #2016-005 (August 22, 2016) Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/ Acting Australian Information Commissioner.

[8] This refers to a framework where privacy is entrenched in the system's design and organizational structure and practices. See: Information and Privacy Commissioner paper on "Privacy by Design" dated September 1, 2013.

[9] Canadian Underwriter (March 30, 2017), Office of the Privacy Commissioner of Canada to fund project on connected cars code of practice.

By

Tamara Tomomitsu, Edona C. Vila

Expertise

Cybersecurity, Privacy & Data Protection, Information Technology, Autonomous Vehicles, Technology, Transportation

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.