# THE CYBERSECURITY IMPLICATIONS OF DRIVERLESS CARS

*Posted on December 14, 2016*

**Categories:** Insights, Publications

Driverless cars have gone from science fiction to fact. While in many respects driverless cars are in their infancy, they are already seen on roadways. For instance, Google's driverless car was reported to have driven over a million miles as of June 2015[1]; Tesla's autopilot software increasingly enables Tesla drivers to rely more heavily on their car's operating system to perform driving manoeuvres;[2] and most recently, Uber started offering customers in downtown Pittsburgh the ability to summon driverless cars.[3]

Early known details about how driverless cars function suggest they will rely heavily on the collection of information in order to understand the surrounding environment and to safely navigate from point A to point B. Driverless cars collect information in various ways, sometimes using their own devices, and sometimes by obtaining information shared with them by other vehicles, connected devices or infrastructure. These vehicles are also expected to collect tremendous amounts of information for safety and even passenger entertainment reasons (as will be discussed further below).

From a cybersecurity perspective, driverless cars present a number of unique considerations, challenges and risks. While many of the issues at play are not necessarily unique to driverless cars, these connected vehicles collect massive amounts of information by design and travel into areas that may often increase the risk of inadvertent disclosure. Moreover, these vehicles may be used to cross borders and enter jurisdictions that require the protection of information in materially different ways.

As the technology continues to develop, manufacturers are encouraged to build sound privacy and cybersecurity practices into the foundation of the design. The former Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian, describes privacy by design as follows:

The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. [Privacy by Design] does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.[4]
This paper examines the privacy and cybersecurity issues concerning driverless cars in the context of the Canadian legal framework applicable to private sector organizations. Manufacturers and developers are urged

to seriously consider Dr. Cavoukian's privacy by design philosophy at this early stage of the driverless car.

**What are driverless cars and how do they collect information?**

A driverless car (also referred to as "autonomous vehicle", or "AV") is generally defined as a motor vehicle with a system that performs dynamic driving tasks with limited human assistance.[5] AVs are generally understood using the following spectrum: Level 0 (no automation), Level 1 (driver assistance), Level 2 (partial automation), Level 3 (partial automation), Level 4 (high automation) and Level 5 (full automation).[6] The Ontario Ministry of Transportation further describes an AV as a driverless or self-driving car that is capable of detecting the surrounding environment using artificial intelligence, sensors and GPS coordinates.

Driverless cars continuously collect information about the environment around them using a variety of sources — including radar, a laser surveying technology called Lidar and three-dimensional maps. To do so, a car's computer utilizes wireless networks to transmit data about the car's surroundings in real time. That data would then go back to the car's computer and possibly also to an external central hub controlled by the manufacturer. With respect to storage of the collected data, one of the options being pursued by various automakers is cloud storage.[7]

Driverless cars must also be able to interact and exchange data with one another in real time. Technology is being developed that would enable driverless cars to communicate with one another and the surrounding infrastructure through sensors that broadcast information.[8] Communication between driverless cars is often referred to as vehicle to vehicle ("V2V") communication. V2V-enabled cars reportedly broadcast a 320-byte message to nearby vehicles up to 10 times per second with basic information including position, acceleration and brake status.[9]

The key data source for driverless cars is Lidar (an acronym for light detection and ranging), which enables driverless cars to perceive their surroundings. Lidar creates a high-resolution, three-dimensional image of the vehicle's immediate environment to a distance of 200 feet. However, in order to create a full understanding of the surrounding environment, Lidar data are integrated with a number of other data inputs. This include digital images, which provide supplemental visual information, such as colour and shape and GPS coordinates, which enable the car to build a precise understanding of its position on the road, and radar and sonar, which helps to detect nearby objects and their proximity.[10]

This data is required to move cars safely though roadways and interact with other vehicles and pedestrians. This basic safety and navigational information is far from the only kind of information collected by driverless cars, however.

In addition to collecting information about the surrounding environment, driverless cars are expected to

increasingly look for information within the vehicle about its passengers, including biometric data.

At the most essential level, driverless cars seek biometric data about drivers in order to enhance the road safety and accident prevention. In a recent report on connected vehicles, the BC Freedom of Information And Privacy Association suggests that car manufacturers may make use of inward facing cameras and biometric sensors to monitor driver alertness and behavior. Semi-driverless cars may utilize eye-tracking, for example, to determine whether a driver is ready to assume manual control of the car.[11]

Modern cars across the autonomous spectrum also typically utilize sophisticated built-in entertainment systems that act as the central hub for a vehicles' multimedia functions, climate control and passenger communication system. These built-in systems are not only used to stream music, content and communications, but also allow users to store personal settings and preferences. More recently, these systems offer services for passenger health and wellness. For instance, some developers are considering connectivity between a car's computer and personal medical devices, such as a glucose monitoring device or a Fitbit.[12]

The connectivity between personal health devices and in-car monitoring abilities of modern vehicles enables manufacturers to collect significant amounts of biometric data from drivers and passengers. The BC Freedom of Information and Privacy Association report referenced above made the following observation concerning health information collection opportunities of driverless cars:

With Bluetooth connectivity, any device can be connected to car systems. This enables carmakers to gather biometric data from drivers and passengers more easily and reliably than via steering wheel or other car-based sensors. For example, heart rate monitors can indicate when drivers are stressed.[13]

Legal Obligations and Liability

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[14] governs protection of personal information in the course of commercial activities in all jurisdictions that do not have substantially similar legislation, as well as protection of personal information related to employees of federally-regulated organizations. Substantially similar legislation currently exists in Alberta, British Columbia and Quebec.[15] Furthermore, to the extent that driverless cars collect biometric and health information, almost every jurisdiction throughout Canada has specific legislation governing protection of personal health information that is collected, used or disclosed by health information custodians.[16]

Some may question the application of privacy legislation to driverless car technology on the basis that the abstract information that a driverless car collects does not easily fit within the concept of "personal" information, which is generally defined as information about an identifiable individual.[17] While the personal preference data collected for use in the vehicle's infotainment system may more easily be identified as "personal information", what about information gathered by a car's Lidar technology?

The Ontario Court of Appeal has found that "personal information" has an elastic definition and should be interpreted accordingly.[18] Driverless cars need to constantly communicate with surrounding vehicles and infrastructure that each collect different types of information. When such information is combined and analyzed, it can present a detailed profile of an individual's lifestyle, habits, health, etc. To the extent that information collected using Lidar about a vehicle's surrounding environment can be connected to the identity of passengers, such information may also qualify as personal information.

Whether a driverless car collects information in order to determine surrounding environment, passenger entertainment preferences or passenger health data, the security of such information is subject to privacy and data security laws.

From a cybersecurity perspective, the most relevant statutory obligations applicable to driverless cars, under PIPEDA, are as follows:

- Personal information must be protected by security safeguards appropriate to the sensitivity of the information.[19]
- Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification, regardless of the format in which it is held.[20]
- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.[21]
- The methods of protection should include (a) physical measures; (b) organizational measures; and (c) technological measures.[22]
- An organization continues to be responsible for personal information it handles, even where that information has been transferred to a third party for storage or processing, and contractual or other means must be used to ensure that comparable levels of protection exist while the information is being processed by the third party.[23]

As discussed in more detail below, these legal obligations present unique issues and challenges when applied to driverless cars.

In addition to these statutory obligations, as discussed in our earlier article, "Cybersecurity – The Legal Landscape in Canada", privacy and data breaches have given rise to a large number of class action lawsuits in recent years, and the common law in this area continues to evolve.

In this regard, interesting questions arise regarding attribution of liability when a driverless car is involved. For example, when damages result from the functioning (or malfunctioning) of a driverless car, who is ultimately

liable? It is an open question as to whether there will or should be any liability imposed on drivers once cars become fully autonomous. Will there still be liability on the vehicle's owner for policy reasons? What about the manufacturer? In 2015, for instance, Volvo and Google both stated that they would accept full liability for accidents involving their driverless cars – though in Volvo's case, only for damages resulting from a flaw in the car's design.[24] What about manufacturers of sensors and other interactivity components such as data hubs? What if a driverless car fails while interacting with a cloud-based service provider, or a 3rd party application, or another driverless car? Accident lawsuits will see a myriad of new defendants who may be involved solely because they act as a link in the data chain between vehicles.

The question of liability becomes even more complicated where a driverless car causes harm on the basis of decisions or actions that were made or coordinated with other driverless cars or surrounding infrastructure. Determining fault for a collision is more complex if the device makes decisions about navigation by first communicating with other driverless cars or infrastructure to coordinate movement.

Existing negligence, product liability and privacy laws may provide some guidance, but several issues will require novel consideration by the courts. Given the rise in privacy and data breach litigation in Canada, and the unsettled state of the law, it is likely that plaintiffs' lawyers will cast their nets widely when searching for liability for damages caused by driverless cars.

**Enhanced cybersecurity risks associated with driverless cars**

In our earlier article "Cybersecurity and the Internet of Things", we discussed the enhanced cybersecurity risk associated with connected devices. The same risks as discussed in that article apply equally to connected vehicles. However, these same risks risks are highlighted in the context of driverless cars by safety considerations and the fact that vehicles are much more mobile than certain other connected devices.

As indicated above, organizations are required to implement security safeguards to protect the personal information that they collect, use, store and disclose. The importance of such safeguards is amplified by the mobility of driverless cars.

Driverless cars are of course designed to travel. These vehicles are expected to share and collect information from a wide array of connected vehicles, devices and surrounding infrastructure across wide geographic ranges and borders. While the evolution in driverless car capability promises many benefits, the greater responsibility and power delegated to driverless cars also creates a greater risk of negative privacy implications, injury, or property damage, if these vehicles fail, mishandle personal information or operate in an undesirable manner.

Given that driverless cars are tantamount to large depositories of data, there are important implications where

these vehicles are used to travel across jurisdictions. It is important for manufacturers and developers to consider the data collection and management practices in the context of differing privacy obligations in the jurisdiction where it collects personal information, and the governing privacy laws in the jurisdictions to which the same data may travel.

Any connected device can potentially be compromised by malicious actors. Therefore, as driverless cars becomes more prevalent, the number of vulnerabilities that can be exploited by the pool of increasingly sophisticated malicious actors will also continue to grow. Moreover, there is a greater risk when driverless cars interact with third-party and cloud service providers. When multiple devices are connected, there is a risk that a weak link in any of them can be exploited to compromise them all.

Furthermore, while loss of privacy, injury or property damage may result solely from the failure of a single device, in other cases it may result from a combination of network vulnerabilities and the intentional malicious exploitation by a third party. In 2015, various media reported on demonstrations conducted by attackers who were purportedly able to disable brakes and interfere with steering of a driverless car.[25]

This heightened risk of harm suggests that more stringent security safeguards will be required for driverless cars in order to comply with legal obligations and reduce potential liability.

**Reducing the Risks**

Given the legal obligations, risks, and uncertainty of liability described above, manufacturers are encouraged to seriously consider the cybersecurity implications impacting driverless cars.

In particular, manufacturers should consider cybersecurity issues from the outset, and build security into the design and development of the product, including by:

Conducting regular security risk assessments or threat impact assessments early in the process;
Considering how driverless cars will interact with other connected vehicles, devices or infrastructure, and options to reduce associated risks;
Taking steps to confirm/ensure that any partners and services providers that driverless cars are able to connect with are appropriately addressing security issues and legal requirements, including implementing appropriate contractual arrangements.
With respect to privacy considerations, developers are also well-advised to conduct a privacy impact assessment to consider the privacy implications and ways to reduce privacy-related risks. In particular, some privacy principles intersect with cybersecurity considerations. For example, the data minimization principle can be applied to reduce risk. If an organization limits its collection of personal information to only what it needs in the circumstances, and disposes of such information (securely) once it is no longer required, this will minimize

the amount of information that is available to malicious actors in the event of a data breach.

Building data security and privacy into the design of driverless cars from the outset can improve functionality and decrease costs, as well as maximizing compliance with legal requirements.

**Conclusion**

Like all transformational technologies, driverless cars come with tremendous opportunities – and risks, including significant cybersecurity and privacy issues. Driverless cars will by necessity collect, create and exchange a massive volume of personal data. All manufacturers involved in making this concept a reality on the road – from vehicle manufacturers to companies who create sensors or connectivity solutions – should be mindful of these issues to ensure that this data is properly collected and protected.

by Geoff Moysa and Mitch Koczerginski

[1] www.techtimes.com/articles/57698/20150603/google-s-self-driving-cars-clocked-up-1-million-miles.htm.
[2] www.tesla.com/presskit/autopilot.
[3] www.bloomberg.com/news/features/2016-08-18/uber-s-first-self-driving-fleet-arrives-in-pittsburgh-this-month-is06r7on. It should be noted that Uber's first driverless cars are still monitored by humans in the front seat, for the time being.
[4] www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf.
[5] O. Reg. 306/15
[6] This automation scale is similar to the U.S. Department of Transportation's National Highway Traffic Safety Administration ("NHTSA") scale, which contains 4 levels ranging from no automation (level 0) to full automation (level 5).
[7] www.business.financialpost.com/fp-tech-desk/the-real-prize-and-threat-of-the-driverless-car-revolution-is-data-the-car-knows-a-lot-about-you
[8] www.business.financialpost.com/fp-tech-desk/the-real-prize-and-threat-of-the-driverless-car-revolution-is-data-the-car-knows-a-lot-about-you
[9] www.business.financialpost.com/fp-tech-desk/the-real-prize-and-threat-of-the-driverless-car-revolution-is-data-the-car-knows-a-lot-about-you
[10] www.eiuperspectives.economist.com/technology-innovation/data-dimension-robotics-and-automation/blog/in

formation-driving-driverless-cars

[11] The Connected Car: Who is in the Driver's Seat,, *BC Freedom of Information and Privacy Association*, at page 41.

[12] The Connected Car: Who is in the Driver's Seat,, *BC Freedom of Information and Privacy Association*, at page 40.

[13] The Connected Car: Who is in the Driver's Seat,, *BC Freedom of Information and Privacy Association*, at page 41.

[14] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

[15] Ontario's health sector privacy legislation has also been declared substantially similar to PIPEDA, but most of the restrictions and requirements only apply to health information custodians.

[16] Every jurisdiction other than Prince Edward Island.

[17] Barbara McIssac, Kris Klein, Rick Shields, *The Law Of Privacy In Canada*, (Scarborough: Carswell, 2012) at 4.1-1.

[18] *Citi Cards Canada Inc v Pleasance,* 2011 ONCA 3, 103 OR (3d) 241 (Ont CA).

[19] PIPEDA Schedule 1, Article 4.7.

[20] PIPEDA Schedule 1, Article 4.7.1

[21] PIPEDA Schedule 1, Article 4.7.2.

[22] PIPEDA Schedule 1, Article 4.7.3.

[23] PIPEDA Schedule 1, Article 4.1.3.

[24] www.bbc.com/news/technology-34475031.

[25] See www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

**A Cautionary Note**

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.