THE COMMON LAWYER

Driving in a Virtual, Electric World

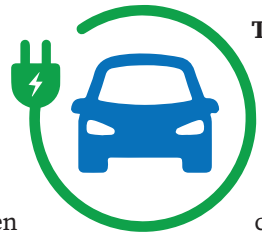
By Justin M Jakubiak and Natalia Sidlar

THE GOOD'OL DAYS OF ROLL-DOWN WINDOWS AND IN-DASH CD PLAYERS (or cassette tapes if you are my vintage!) are long gone. While power windows have been around for decades, the vehicles that get us from point A to B have vastly improved and now often come standard with Bluetooth, WiFi, charging pads, navigation and much more – they are basically computers on wheels.

Technology hasn't stopped at creature comforts, it has also revolutionized the way many new vehicles are powered. The manufacture, purchase and sale of EVs in Ontario have steadily increased year over year. Luxury and mainstream brands alike have added EVs to their lineup (no doubt to compete with Tesla's virtual monopoly of the space), with many brands pledging to go entirely electric over the next several years.

As the vehicles and the landscape in which they operate change at a frenetic pace, one must ask: has the automotive industry prepared itself for the electric new world? Are car dealers and their staff ready for this new world and the responsibility that comes with increasingly 'smart' cars?

The rise of EVs and vehicles which are more computer than engine raise a number of privacy and cybersecurity concerns/threats that dealers must prepare for in order to ensure continued excellence in service and client experience – and equally as important – future OMVIC/MVDA compliance.



The Rise of EVs and Increasing Technology

Whether you like it or not, they are coming. No, we are not referring to the robots that are coming to take our jobs; but 'smart' vehicles and vehicle technology that connects us more and more to the world around us.

In May of this year it was announced that the federal and provincial governments are going to provide $1-billion to Chrysler and Dodge factories in Brampton and elsewhere in Ontario to build the next generation of hybrid and EVs. In July it was also reported that construction on a new battery component facility in Kingston, Ontario will commence in 2023. The facility will supply parts for electric

vehicles and will hopefully, according to Prime Minister Justin Trudeau, make Canada a global leader in EVs.

EVs often look funny, they sound weird (or make no noise at all) and the debate continues to rage as to whether they are in fact better for the environment – that said, Tesla is a prime example of why we can't ignore the nascent electric age of motor vehicles. Taking a stroll through Yorkdale shopping mall really brings this home: Lucid has followed Tesla's lead and now has a showroom in the mall, and VinFast is currently building out a space which looks like it may be bigger than both the Tesla and Lucid stores combined. Clearly, not only are vehicles and their technology changing, but the entire retail landscape as well.

Fart Mode and Your Shopping Habits

Electric vehicles and technology go hand in hand. If you have ever driven an electric vehicle, you will have likely noticed that it presents much more like a computer than a traditional vehicle. Justin's 6 year old son's dream of a green Lamborghini was quickly sidelined when he sat in a Tesla and realized he could

play games on its computer sized screen and that it had a fart mode (yup, the fart mode allows you to use any of the car's speakers to make farting sounds!).

Like your mobile phone, your Tesla, along with most modern vehicles, is increasingly connected to the world around it and is constantly amassing information about you, your vehicle, where you live, your daily habits and more. While information is power, and all of this collected and stored information can be used by manufacturers to improve their product and the driver's user experience, there is a big and looming dark side which cannot be ignored.

This detailed digital record of your daily habits is incredibly valuable – to both of society's good and bad actors. To know your every move is something most marketers would pay a fortune for in order to improve their marketing efforts and to sell you more. But who owns the information that is collected by your vehicle? Do you agree that it can be shared – and if so, to whom? Would you like your vehicle to suggest locations, destinations and shops based on your past habits? If not your vehicle, can third parties, through your vehicle, advertise locations they think you may be interested in based on your past habits?

Like all information, your personal vehicle information likely has incredible utility, and if used correctly, may vastly improve your vehicle experience – such as directing you to travel a route with less traffic, or with no tolls, or with better scenery. However, where you do your shopping, how often you buy groceries, when and what times you frequent your local LCBO is also very private and personal information.

When there is information that people want and will pay for, a landscape is created for bad actors to do what they need to do to obtain access to that information at any cost.

Who owns the information stored in a vehicle? The driver? The Manufacturer? The Dealer?

The pressing questions raised by this article are why many organizations, like the Canadian Automobile Dealers Association, and its American counterpart, the National Automobile Dealers Association, have been working hard to think about the ethical and practical issues that arise with the advances in technology. They have recently developed data sharing principles for manufacturers and dealers to help ensure legal and regulatory compliance, protect consumers, and promote trust in the automotive ecosystem.

Essentially, these principals are an acknowledgement that by the very nature of the modern automotive industry, there is a ton of data which will regularly flow between dealers, manufacturers, their respective systems and the vehicles themselves. This data has to be organized, has to be secure and has to be shared in a responsible and ethical manner that protects all parties that come into contact with such data.

A Dealer's Responsibilities

As a dealer, what information are you knowingly or unwittingly becoming a custodian of in the normal course of your operations? What can you use and what can you profit from? What must you protect? As vehicles become more sophisticated and have more technology, so too will your dealership. Service will migrate from routine oil and fluid checks to routine computer diagnostics and the fixing of bugs and other technical glitches. One can imagine a world where a dealership will have to download some or all of the information that is stored on a customer's vehicle in order to assist in a particular diagnosis.

In response to these changes, modern dealers will have to amend their customer facing agreements to account for this information transfer. Customers will want to know that their personal information is safe and secure, and won't be sold to third parties without their acknowledgement and consent.

Employment agreements and policies will also have to be amended to ensure that

salespersons and mechanics are aware of and understand their legal and ethical obligations when they, in the course of their duties, come into contact with a customer's personal information.

Hackers, Viruses and other Threats

Just like a cellphone or a laptop, modern vehicles are at risk of being hacked or infected with a virus or some other type of malware. One such gateway for these risks are applications that allow an owner to control and access their vehicle from their computer or smartphone. While such applications are convenient, there is a real risk that data can be breached and even the vehicle itself could be remotely accessed and controlled.

Another, and possibly riskier threat, lies with public charging stations that essentially connect a vehicle to the internet. Not only is the EV at risk of being hacked, but any device connected to the EV (such as a cellphone) may also be at risk of hacking threats – arguably, any personal data within the car and within a cellphone is under threat. Not only can banking information, personal identification, passwords etc. be stolen, but driving routes and habits as well.

These cybersecurity threats present concerns for both manufacturers, car dealers and consumers. While manufacturers will need to focus on encryption, consumers may have to be more mindful of how, when and where they recharge their EV or service their 'smart' vehicle. Car dealers, much like retailers of used computers and cellphones, will have to scrub used vehicles of personal information before they are resold, and may also need to consider running a full virus diagnostic to detect malware that could compromise future privacy – in the near future, it will likely no longer be enough for a dealer to simply review the vehicle for mechanical and structural flaws before selling it.

Consumers interested in EVs will inevitably begin asking questions about battery health, software issues and whether the vehicle had previously suffered significant trauma to its electronic brain. Has the computer been rebuilt or rebooted? Have all updates been completed? Is the anti-virus software current? Perhaps when it comes to marketing, dealers may have to state and/or otherwise inform a potential consumer about the technological health and past of the vehicle.

Data Sharing Agreements

In addition, at some point, dealers and salespeople may have to consider their role (and potential liability) in keeping drivers and their personal information safe from a cybersecurity perspective. As mentioned earlier, as vehicles get smarter, the information collected by a dealer will inevitably increase. Dealers will need to increase their cybersecurity and privacy measures; one way is for dealers and consumers to consider entering into Data Sharing Agreements which can limit how and in what ways a dealer can use and share the personal information collected from smart vehicles. While a consumer may want information about the maintenance and overall health of their vehicle shared with the dealer, they may want other information ignored or destroyed by the dealer if inadvertently collected.

Adapting to the Electric and Virtual Times

The increase in the sale of smart vehicles and EVs, and the increasing shift to online vehicle sales, all requires the law to adapt to the changing landscape. OMVIC and the MVDA will have to change to address these changing paradigms, and ensure they can continue in their public protection mandate.

One hopes that OMVIC will be able to adapt to the upcoming changes as well. The industry will need an organization that is flexible and mindful of the agility required to stay current and to assist dealers and consumers alike in navigating this new word.

Conclusion

Like all change, the changes in the automotive industry comes with its pros and cons. There is no doubt that EVs and smart cars will have huge benefits, but the associated disadvantages will have to be considered and managed.

Dealers and consumers must equip themselves with knowledge and must implement necessary protocols surrounding this electronic, virtual world. Both buying an EV and buying it online comes with two separate opportunities for fraud to take place, not to mention the amount of information transferred in the process which is subject to hack and misuse.

The manufacturers, dealers, consumers and OMVIC will all need to evolve and work together in order to protect the industry as a whole.

Justin is a Partner with Fogler, Rubinoff LLP and is recognized by the Law Society of Ontario as a Specialist in Civil Litigation – most importantly, he loves cars and the automotive industry, representing auto clients throughout Canada. Natalia is a new member of the firm's automotive group and has a passion for all things automotive and transportation related.