Will Privacy Be the Next Moral Crumple Zone?[1]

Ian Kerr[2] and Jason Millar[3]

Policy Provocation

The automotive industry's aversion to liability for accidents resulting during the engagement of SAE Level 2/3 automation is on a collision course with privacy. Just as 'crumple zones' are designed to absorb the lion's share of energy in a physical impact, drivers' privacy interests in semi-automated driving modes are poised to bear the brunt of social impacts. Industry's desire to offload liability to drivers will result in an increasing reliance on *internal sensors* to track human activity *inside* automated vehicles. Increased monitoring of the shared driving responsibility that lower-level automation requires will therefore pose a novel threat to the privacy of drivers and passengers. The use of internal sensors will increase the overall personal information collection payload with more and more personal data being collected and controlled by the automotive industry. It will also affect the nature and quality of privacy afforded to individuals inside their vehicles, which raises pressing questions about how much and what sorts of information can be collected and retained, who, if anyone, owns that information, and who is permitted access to it.

The means by which manufacturers attempt to avoid liability will also exacerbate safety risks on the road. Marketing language promoting SAE Level 2/3 automation differs significantly from the actual legal disclaimers and notices a driver must accept when operating the vehicle, which can amplify "automation bias"—i.e., the errors drivers tend to make in automated decision-making contexts that can cause them to "over-trust" a vehicle's ability to carry out the driving function on its own.

The risks associated with automation bias and privacy can both be significantly reduced through ethical design choices, especially as automation proceeds towards SAE Level 5.

---

[1] We owe the gorgeous concept of a 'moral crumple zone' to Madeleine Claire Elish who introduced this concept in support of her hypothesis that "the human in a robotic system may become simply a component … that is intended to bear the brunt of the moral and legal penalties when the overall system fails": https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757236

[2] Dr. Ian Kerr is the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa's Faculty of Law.

[3] Dr. Jason Millar is an Interdisciplinary Postdoctoral Fellow at Stanford University's McCoy Family Center for Ethics in Society and Apple, and a Research Affiliate at the Center for Automotive Research at Stanford.

Objectives

1) To illustrate how manufacturers' current means of avoiding liability for SAE Level 2/3 automated vehicle crashes amplifies safety risks associated by amplifying automation bias.
2) To demonstrate how the threat of liability for SAE Level 2/3 automated vehicle crashes generates novel privacy concerns.
3) To distinguish between internal and external vehicular privacy and the different challenges that each pose to access to information, data collection, use, and disclosure.
4) To illustrate different design options for combating problems associated with automation bias and driver inattention and their respective impact on privacy.
5) To suggest that privacy can and actually should be enhanced through design—especially as automation proceeds to SAE Level 5.

When Liability and Privacy Collide

The looming threat of legal liability for SAE Level 2/3 automated vehicle crashes threatens road safety and generates novel privacy concerns. Consider the following Case Study.

Case Study: The Casualties of Teslean Doublespeak

It was a clear spring day in May, 2016, a perfect day for driving, when Joshua Brown took 'Tessy' out for her last cruise. The remains of Brown's Tesla Model S had to be towed from the accident scene, while the former Navy Seal's bodily remains, cremated. Trusting that Tessy's autopilot would steer clear of any road hazards, Brown had taken his hands off the wheel and was not paying attention when his car slammed into a semi-trailer. His Telsa's external sensors were unable to distinguish between the pale blue sky and the off-white tractor trailer that had made a left turn into the road in front of him. Brown, a Tesla aficionado, had logged more than 45,000 miles in his Model S in less than 9 months; many of them driving hands-free, as documented in the two dozen YouTube videos that he posted online (Brown, YouTube, 2016). His cultish trust in Tessy was clear—according to a report issued by the National Transportation Safety Board (NTSB) one year later, Joshua Brown had only placed his hands on the wheel for a total of 25 seconds over the course of 37 minutes of cruising. Of those 25 seconds, his hands only touched the wheel in one-to-three second intervals, which he did as a means of circumventing repeated audio and visual warnings from the vehicle's dash monitors. While the crash was originally attributed to human error, NTSB subsequently determined that: "The combined effects of human error and the lack of sufficient system controls resulted in a fatal collision that should not have happened." (Marshall, WIRED 2017)

While the NTSB acknowledged the manufacturer lacked "sufficient systems controls" it did not prescribe what systems controls are required, leaving it to industry to sort out for itself. And, although the report deals with the issue of driver inattention, NTSB does not deal with the larger issue: the well understood psychological disposition known as "automation bias." Automation bias "refers to a specific class of errors people tend to make in highly automated decision-making contexts, when many decisions are handled by automated aids (e.g., computers), and the human

actor is largely present to monitor on-going tasks" (Skitka, 1999). One of the most typical errors associated with automation bias is the tendency to over-trust an automated system despite being fully aware of its defects, and of the potential risks associated with over-trust. Automation bias can therefore be triggered by companies that intentionally over-sell the automation capabilities of their vehicles.

Tesla and its CEO, Elon Musk, seem to have taken this very tact in the schism between their sales talk and their legal language.

In what might be coined "Teslean Doublespeak", at one and the same time, Tesla claims that its driving features are worthy of being called an "autopilot", yet that the driver, while in autopilot mode, must perform every mental driving task with her hands on the wheel, with the exceptions of actually steering the vehicle, braking and accelerating. One need only engage in the schizophrenic exercise of parsing Tesla's marketing and legal language at the same time to see how the risk of automation bias is elevated. CEO Elon Musk has been making extremely bold marketing statements with great regularity for several years about his cars' ability to drive themselves. Claiming in 2015 that "[i]t's a much easier problem than people think it is," Musk promised that "we will have complete autonomy in approximately two years." (Korosec, 2015). He doubled down on this claim in January 2017 promising "full self-driving capability" in "3 months maybe, 6 months definitely" (Fagella, 2017). These (over-)confident reassurances, spread like wildfire by fans and aficionados using social media, are reinforced by automotive features marketed as "Autosteer", "Auto Lane Change", "Autopark" and "Traffic Aware Cruise Control."

Meanwhile, the legal language associated with these Tesla products is a stunning example of Orwellian doublespeak. For instance, the legal language explicated in the Tesla Model S Owner's Manual (Tesla, 8.0) regarding the feature called "Autosteer" reads as follows:

> Autosteer requires you to hold the steering wheel. If it does not detect your hands on the steering wheel for a period of time, a flashing white light appears around the instrument panel and the following message is displayed on the instrument panel.

The doublespeak in the "Auto Lane Change" is equally baffling:

> Warning: Never depend on Auto Lane Change to determine an appropriate driving path. Drive attentively by watching the road and traffic ahead of you, checking the surrounding area, and monitoring the instrument panel for warnings.

In light of the misleading product names and the extensive and relentless company hype—even if drivers are obligated to read as far as page 74 of the online Owner Manual—how could Joshua Brown and others be expected to fully comprehend that Autosteer requires the driver to hold onto the steering wheel and Auto Lange Change cannot be depended on to change lanes?

Joshua Brown is not the only casualty of Teslean Doublespeak. Privacy is another. The spectre of liability for AV/CV fatalities, especially in light of the first Tesla autopilot crash, has caused the

AV/CV industry to respond by populating its cars with *internal* sensors. Unlike the many external sensors necessary to automate the driving function, the sensors inside the car have an entirely different purpose: surveillance of the human driver. The legal strategy behind this surveillance is to offload liability for the shared driving function to the human driver.

Placing the focus on driver inattention and human error raises novel privacy claims of various sorts, depending on how those systems are designed. For example, Tesla, Audi and others currently focus their internal sensors on the steering wheel. Audi's system requires the driver to touch base with the steering wheel every 15 seconds, failing which as series of irritating audio signals will cue the driver. If the driver fails to respond, the vehicle will automatically slow to a stop. After its first fatality, Tesla upgraded its system to do the same. The automotive industry, as a whole, may be moving towards even more sophisticated surveillance systems. For example, Cadillac's Super Cruise uses micro cameras and infrared lights that track head position to determine where the driver is looking. The newer systems also use facial recognition software in order to help detect whether the driver is paying attention. A failure to meet Cadillac's proxies for attention (eyes aimed at the road) will prompt the driver. A continued failure in gaze location will escalate alerts and illuminate "a steering wheel light bar, visual indicators, tactile alerts in the seat and audible alerts. If the driver does not respond, the vehicle is brought to a controlled stop" (Shepardson, 2017). As is evident from the NTSB report on the Tesla crash, many of these systems log all of this information, which is available for analysis post-crash, much like the black box (flight recorder) in an airplane.

Policy-Relevant Questions:

1) Does the existence of automation bias require some form of regulation in the AV/CV context? Are internal sensors the best solution?
2) How might internal sensors be used in a more privacy friendly manner?
3) If we were to shift liability considerations from the driver to the manufacturer, what policies or guidelines might better prevent over-trust in SAE Level 2-3 automation? Is additional consumer protection legislation necessary?
4) Should attempts to 'trick' or circumvent internal sensors be illegal?
5) With respect to internal vehicle sensors, what is the relationship between privacy and safety?
6) With respect to internal vehicle sensors, when does public safety trump individual privacy?

Internal vs. External Privacy Interests

Some policymakers have argued that AV/CVs do not raise novel privacy issues because the main risks associated with geo-locational tracking already present themselves through our use of other devices such as GPS, smart watches and mobile phones.

As a counter-consideration, it is useful in the AV/CV context to distinguish between two different privacy interests: external and internal. *External privacy interests* are those associated with external sensors used to facilitate the automated driving task. These include not only geo-locational services but also other sensors used to monitor external objects on and around the

roadway, including people. Although they have the potential to implicate privacy, current external sensor systems do not seek to identify people who are outside the vehicle, scrutinize their activities, or collect/use/disclose any information about them. The data are used simply to detect whether humans, animals or other objects are, or risk being, within the path of the vehicle. Although some regulators (German Federal Ministry of Transport and Digital Infrastructure, 2017) have speculated about the implications of future sensors that could distinguish between people and things—perhaps even to the point of identifying individuals as belonging to certain groups or categories—that is not the current reality. Currently, external sensors are not aimed at surveillance or any kind of social sorting. The German approach aims to promote ethical design that would avoid creating such risks in the future.

Internal privacy interests, by way of distinction, are those associated with internal sensors used to monitor human activity inside of the vehicle. Such monitoring is potentially problematic from a constitutional law perspective since the Supreme Court of Canada (SCC) has, for many years, held that people are afforded some level of privacy inside of their vehicles (*R v Belnavis,* 1997).[4] Data collected from "always-on" internal sensors under the auspices of detecting driver inattention threaten the privacy interests of drivers and passenger. This will create a novel privacy claim and generate additional tension between privacy and public safety as driver/passenger surveillance is heightened to previously unimaginable levels.

As we have seen, some companies are already moving towards the use of cameras, infrared, and facial recognition. These sensors and more sophisticated ones yet to be developed have the potential to reveal much more than just geolocation. These technologies have the capability to identify individuals and determine whether they are members of identifiable groups. They also have the ability to scrutinize driver and passenger activities and interactions, collecting/using/disclosing information about people while they are inside their cars. Although such sensors might be justified for certain narrowly specified purposes under certain narrowly specified conditions, the fact that they are monitoring human activity in privately owned vehicles gives rise to a legitimate and somewhat novel privacy interest while, at the same time, generating a false sense of trust that the vehicle is performing the entire driving task.

Access to AV/CV Sensor Data

Given the differences between internal and external privacy interests, it is likely that access to AV/CV sensor data will very much depend on who is seeking it, and what kind of sensor data they are seeking access to. The concept of "data ownership" with regard to the information generated by mobility networks will prove challenging. Indeed—given the different roles and relationships of data-generators, data-collectors, data-users, and data-subjects, as well as the different private and public layers of oversight of mobility networks, it may be more useful to speak simply in terms of who holds or controls the information and who should have lawful access to it.

[4] Although vehicles on public roadways are said to give rise to a lower expectation of privacy than, say, a person's home: *R. v. Wise,* 1997.

It is useful to consider a couple of examples.

1. Public Sector Access to Internal AV/CV Sensor Data

As discussed, some internal AV/CV sensor data collected by manufacturers will attract a higher privacy interest than most of the human activity captured by external sensors related to the driving function. This is in part because external sensors generally monitor unidentifiable individuals in public spaces.[5] To the extent that internal sensors record data about the private activities of identifiable individuals within the confines of a privately-owned vehicle, the data-subject—whether sitting in the driver seat or elsewhere in the vehicle—likely holds a reasonable expectation of privacy (*R. v. Belnavis*, 1997).[6]

Thus, in the context of public sector access to internal sensor data (including access by law enforcement, public safety, municipal planning, or other governmental oversight bodies), the monitoring of human activity inside an AV/CV will almost certainly trigger the constitutional right to privacy guaranteed by way of the search and seizure provision in section 8 of *The Canadian Charter of Rights and Freedoms*—so long as the data subject can demonstrate a "reasonable expectation of privacy."[7] As discussed below, this will affect whether and by what means public sector actors may gain access to the data regardless of who owns it.

When one further considers the matter from an informational (rather than a territorial) point of view, questions about public sector access to internal AV/CV sensor data are not just about what happens within the confines of the physical interior of the vehicle but also in the broader surveillance activities occurring by virtue of the vehicle's connection to online networks. When one takes connectivity into account, it is likely that newer cases dealing with cellular networks and service/platform providers are even more applicable than the traditional search-of-vehicle cases.

Consider, for example, *R. v. Spencer* (2014). This SCC decision sought to determine whether police could request subscriber information from an online service provider in order to identify an individual engaging in certain online activities on a voluntary basis, without prior judicial authorization. The Supreme Court unanimously ruled that obtaining such information without a warrant infringed the *Charter's* guarantee against unreasonable search and seizure. The SCC held

[5] It is crucial to recognize that many human activities in public places still attract a reasonable expectation of privacy (Timan, Newell and Koops, 2017). But most privacy law is concerned only about identified or identifiable individuals.

[6] Novel questions will arise if the driving model shifts significantly towards autonomous fleet vehicles, depending on whether they are licensed or not. While privacy expectations are reduced in today's publically licensed taxis, it is possible that Uber and other types of unlicensed/privatized ride-sharing systems might attract a greater expectation of privacy.

[7] It has been several years since scholars and courts started evaluating the possibility of a reasonable expectation of privacy in vehicle sensors such as the data recorded by a vehicle's airbag sensing diagnostic module (Scassa, 2014). Cameras, infrared and facial recognition systems in the interior of a vehicle would obviously attract an even great privacy expectation.

that "[d]isclosure of … information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that a [service provider] voluntarily disclose such information amounts to a search." The result in *Spencer* is that police and other public-sector actors will now require a warrant in order to obtain subscriber information and other personal information (except in exigent circumstances). Consequently, the practice of networks and other service providers voluntarily providing this information must come to an end. More recently, the SCC has also affirmed that even text messages sent across an open network are considered private even after they are received by another person, in which case the police cannot have access to them without a warrant: *R v. Marakah* (2017).

These and other cases provide a solid foundation for the likelihood that internal AV/CV sensor data will be subject to the data-subject's reasonable expectation of privacy, thus triggering the *Charter of Rights and Freedoms*. Consequently, there is good reason to think that AV/CV internal sensors used as a surveillance mechanism to enforce driver attention will create novel privacy risks in vehicles.[8] The likely result of this is that warrants and court orders will be necessary for public sector access to internal sensor data.

2. Private Sector Access to Internal/External AV/CV Sensor Data

Private sector access to internal AV/CV sensor data is not generally subject to constitutional scrutiny. Collection, use or disclosure of such data may, however, be subject to Canada's federal data protection law (PIPEDA, 2000) and substantially similar provincial data protection laws. In order to be subject to these laws, the data must comprise personal information about identifiable individuals. With limited exceptions (e.g., an investigation regarding the violation of a federal or provincial law), privacy laws generally require the data subject's consent in the collection, use or disclosure of personal information. In order for such consent to be effective, it must be reasonable to expect that the data-subject would understand the nature, purpose and consequences of the collection, use or disclosure.

One of the key issues sure to arise in the AV/CV context is how broadly automotive manufacturers can share personal information collected by way of AV/CV sensors with other private sector entities. As a preliminary matter, because the relevant threshold is whether the information is "personal information" rather than whether it attracts a "reasonable expectation of privacy", it is unclear whether the internal/external sensor distinction discussed above will be helpful in delineating the kind of sensor data that carries a privacy interest. It may be that *all* sensor data that is personal information will be treated the same.

In any event, once an organization obtains consent to use and disclose its sensor data, it can grant access to other private sector entities. The means of gaining consent is usually by way of standard form agreements, terms of service, and privacy policies connected with the sale or lease of the vehicle. Until recently, this meant that data collectors—in this case the automotive industry—

[8] It is unclear whether the above analysis would apply in the case of future case of SAE Level 2-3 AV/CV used for Uber or other ride sharing services that render the vehicle more like a public space.

could write their own rules about who gets access and what those with access are allowed to do with it. The take-it-or-leave it nature of these agreements has the practical effect that drivers' and passengers' only choice is to agree to the terms or else find another means of mobility. Accordingly, consent to the sharing (read: selling) of sensor information and other valuable mobility data is usually an upfront requirement in the manufacturer's contract of sale or lease. Up until now, data collectors in and outside of the automotive industry have used contracts for the sale of goods or services in this way as a means of circumventing obligations that they would otherwise have pursuant to private sector privacy laws (Kerr, 2006).

Important policy issues arise. Should the automotive industry (and other large data collectors and platform providers) be permitted to collect, use and disclose internal and external sensor data however it likes, simply by specifying as such in their contracts? Does this leave consumers with any choice? How might this possibility impact broader mobility rights?

From the consumer protection perspective, there is some hope that recent developments at the SCC might limit the automotive industry's ability to "contract-out" of privacy protections otherwise guaranteed by statute. In *Douez v. Facebook* (2017), the SCC examined Facebook's requirement that users must consent to a jurisdiction clause requiring them to resolve any dispute they had—big or small—only in its home base in California. Although Douez and others clicked "I agree" to its terms, the Court found that the jurisdiction clause was unenforceable. The Court concluded that service providers will not be able to dictate all of the terms, especially where such terms are not in the public interest or are contrary to public policy.

AV/CV policymakers will have to think carefully about whether they want to leave privacy in the hands of industry and whether sector specific legislation is desirable in light of design developments around sensor capabilities.

Privacy Need Not Be a Crumple Zone

Having discussed how the automotive industry's desire to circumvent liability motivates the circumvention of privacy and some possible and actual responses from courts and legislatures, it is worth noting that privacy need not be a crumple zone. Some manufacturers recognize privacy protection is a good business practice and are incorporating privacy and a broader set of ethical principles into the design of their vehicles.

Whether industry chooses to embrace privacy protections or not, the General Data Protection Regulation (GDPR), coming into effect in May 2018, requires manufacturers operating in Europe to implement data protection by design and by default into their processes and products. This means that automotive products and processes will be required to build strict privacy settings as the default mode of operation, and that control over the use of data must remain in control of the individual to whom that data relates. Many non-European manufacturers have chosen to adopt the GDPR standards as their default *modus operandi* in anticipation of future domestic regulation seeking to meet the adequacy requirements of the GDPR.

Already known as a global leader in privacy and data protection, Canada is sure to follow suit. Privacy by Design, a concept initially developed in Ontario, sets out seven principles that ought to be taken into account early on and throughout the design process. They include:[9]

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

From the perspective of Level 2-3 AV/CV internal sensors, a privacy by design approach could mean that collected data only be stored or shared according to strict rules that are clearly communicated to the driver. It might also mean that certain data would be off limits to manufacturers, using technology to limit access to investigators in situations where the data was required as evidence in driving events or crashes that increase risks to safety. To continue the example from above, privacy by design might also render data collected by cameras, infrared, and facial recognition systems unidentifiable while still achieving the aim of monitoring driver inattention. This would allow crash investigations to move forward without implicating the privacy of individuals who have not yet been found responsible for any wrongdoing.

One need only consider the privacy implications raised by the practically immediate release of detailed video footage by the Tempe Police Department after the first Uber/Volvo fatality (Tempe Police, 2018). This video identified the Uber test driver, leading to the revelation that she was a convicted felon. The social stigma connecting her criminal past with her participation in the monumental, first-ever AV/CV pedestrian fatality will undoubtedly affect her future life chances and opportunities—even though it could very well turn out that she was not at fault. The key insight here is that a driver's privacy—which in this case was clearly implicated as a result of the capture and release of internal AV/CV sensors data—could just as easily have been protected without any increased risk to safety, through the simple implementation of a facial obscuring algorithm.

The lesson here is: even when tensions appear to exist between the two, safety and privacy are not necessarily at odds with one another.

SAE Level 4-5 Automation Can and Should Become More Privacy Friendly

We have suggested throughout that privacy risks are becoming a crumple zone for liability arising from SAE Level 2-3 automation even though there are means of achieving privacy by design. We

[9] For an elaboration on each principle see Cavoukian 2011.

end with the counter-intuitive provocation that privacy can and actually should be enhanced though design—especially as automation proceeds to SAE Level 5.

Once the dynamic driving task is highly automated, there will be less need, from a liability perspective, to focus on human activity inside the vehicle. As automation improves and safety is enhanced, there becomes more and more reason to monitor the performance of the vehicle and its operations, not its passengers. Enhanced cybernetic feedback is necessary to move AV/CV from SAE Level 4 up to Level 5. But, as the previous section suggests, ethical design choices can achieve these ends with less focus on human activity and a greater focus on the functioning of the vehicles and the movement of critical data through mobility networks.

An important lesson for designers and regulators to remember is to avoid function creep (Jacobs, 2016). One must keep in mind that the original purpose associated with using internal sensors in SAE Level 2-3 AV/CV is specifically to address driver inattention and automation bias. Using internal sensors for any other purpose would be a privacy infringement. Likewise, adding internal sensors or improving their capture once driver inattention and automation cease to be relevant issues would require and entirely new justification and fresh consent.

Thus, though there will be overwhelming big data incentives to further populate the inside of cars with more and more sensors and monitoring devices—likely tied to conveniences associated with new services that they help to provide—from a privacy perspective, the goal of full automation should carry with it the further goal of ensuring the privacy of AV/CV users and eliminating associated risks.

References

Brown, J. (2016). “Joshua Brown.” *YouTube.* Online: https://www.youtube.com/channel/UCLqNcKzWLAVb1Ez6SbshI7g

Canadian Charter of Rights and Freedoms (1982)

Cavoulkian, A. (2011). “Privacy By Design” Online: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

Douez v. Facebook, 2017 SCC 33

Fagella, D. (2017). “Self-driving car timeline for 11 top automakers” VentureBeat. Online: https://venturebeat.com/2017/06/04/self-driving-car-timeline-for-11-top-automakers/

Federal Ministry of Transport and Digital Infrastructure. (2017). *Ethics Commission: Automated and Connected* Driving. (June). Online:https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile

Jacobs, M.F.G. (2016). “Function Creep in Surveillance Situations: Identifying control paradoxes through agency and power relations using ANT.” *Faculty of Humanities, Master Thesis*. Online:https://dspace.library.uu.nl/handle/1874/336638

Kerr, I. (2005). “If Left to Their Own Devices ... How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy.” In M. Geist (ed.) *In the public interest: the future of canadian copyright law*. (Irwin;). Online:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=902448&rec=1&srcabs=1095876&alg=1&pos=4

Korosec, K. (2015) “Elon Musk Says Tesla Vehicles Will Drive Themselves in Two Years” Fortune. Online: http://fortune.com/2015/12/21/elon-musk-interview/

Marshall, A. (2017). “Tesla bears some blame for self-driving crash death, feds say.” *WIRED* (Sept. 13). Online:https://www.wired.com/story/tesla-ntsb-autopilot-crash-death/

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

R. v. Belnavis [1997] 3 SCR 341

R. v. Marakah, 2017 SCC 59

R. v. Spencer, 2014 SCC 43

R. v. Wise [1992] 1 SCR 527

Scassa, T. (2014). “The Reasonable Expectation of Privacy and Your Car's Airbag System” Online: http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=172:the-reasonable-expectation-of-privacy-and-your-cars-airbag-system&Itemid=80

Shepardson, D. (2017). “Tesla, others seek ways to ensure drivers keep their hands on the wheel.” *Reuters* (June 23). Online:https://www.reuters.com/article/us-usa-autos-selfdriving-safety/tesla-others-seek-ways-to-ensure-drivers-keep-their-hands-on-the-wheel-idUSKBN19E1ZA

Skitka, L. (1999). Online:https://lskitka.people.uic.edu/styled-7/styled-14/index.html

Tempe Police Department Video Footage (2018). Online: https://twitter.com/TempePolice/status/976585098542833664

Tesla Model S Owners Manual. 8.0. Online: https://www.tesla.com/sites/default/files/model_s_owners_manual_north_america_en_ca.pdf