Canadian Journal of Law and Technology

Volume 17 | Number 1 Article 4

6-1-2019

Big Brother Riding Shotgun: Internal Surveillance of Semi-Autonomous Vehicles and its Effects on the Reasonable Expectation of Privacy

Tunca Bolca
Faculty of Law, University of Ottawa

Big Brother Riding Shotgun: Internal Surveillance of Semi-Autonomous Vehicles and its Effects on the Reasonable Expectation of Privacy

Tunca Bolca*

I. INTRODUCTION

The makers of autonomous vehicles (AVs) claim that their vehicles will reduce traffic accidents by 90 per cent and save millions of lives.[1] Although this is yet to be proven, even if these new generation cars are made to be everything that the carmakers claim, accidents will still happen. Now, as the technology is progressing, governments and scholars are trying to come up with solutions to many legal, ethical and sociological problems the AVs will bring along.

Full autonomy is still far away, but semi-autonomous cars, which are listed as level 2 and 3 at the Society of Automotive Engineers' (SAE) Levels of Autonomy,[2] are now available for public use. Level 2 is listed as "partial automation", where the "[v]ehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times."[3] Level 3 means "conditional automation" and although a driver has to be present, the driver is not required to monitor the environment at all times. However, the driver must still be "ready to take control of the vehicle at all times with notice."[4]

One of the major challenges of this technology is its impact on privacy. AVs produce and collect a lot of data that contain personal information through GPS localisation, cameras, sensors, *etc*. Most of this data production is done "externally"; the vehicle uses sensors and cameras to monitor the road and other factors (e.g. other vehicles, pedestrians) thus creating a lot of data concerning the

---

* LL.B, LL.M (Private Law), LL.M. with Concentration in Law and Technology (cand.), University of Ottawa, Faculty of Law. The author would like to thank professors Ian Kerr, Teresa Scassa and Elizabeth Judge of the University of Ottawa for their support and guidance.

1 Adrienne LaFrance, "Self-Driving Cars Could Save 300,000 Lives Per Decade in America", *The Atlantic* (29 September 2015), online: < www.theatlantic.com/technology/archive/2015/09/self-driving-cars-could-save-300000-lives-per-decade-in-america/407956/ > .

2 United States Department of Transportation, National Highway Traffic Safety Association, "The Road to Full Automation" (accessed 2 April 2019), online: < www.nhtsa.gov/technology-innovation/automated-vehicles-safety > .

3 *Ibid.*

4 *Ibid.*

vehicle's interaction with traffic and the surroundings. GPS localisation data can also be considered as external, even though the potential harm of the data is towards the privacy of the driver, the GPS system tracks the vehicle's movements and does not collect any information regarding the interior of the vehicle. The collected data through the vehicle's interactions with the world outside the vehicle present privacy concerns for both the driver of the vehicle and the parties the car detects through its technology, such as other drivers or pedestrians. However, this article will focus on a new practice that produces more challenging privacy issues in the current level 2 and 3 autonomous vehicles.[5] Due to the level of the technology in these vehicles, the automakers are designing systems to monitor the interior of the vehicle to detect driver engagement in order to shift the blame to an inattentive driver in case of an accident. This practice of internal surveillance of the vehicle raises novel privacy concerns for the drivers and passengers of these vehicles.

In Canadian jurisprudence, it has been accepted that individuals have a reasonable expectation of privacy in their vehicles and are protected from unreasonable searches of the state under s. 8 of the *Canadian Charter of Rights and Freedoms* (*Charter*).[6] This article examines the concept of internal surveillance and identifies how the individuals' reasonable expectation of privacy will be affected by the introduction of semi-autonomous vehicles that use internal surveillance methods.[7]

II. INTERNAL SURVEILLANCE IN LEVEL 2 & 3 AVS AND THE REASONABLE EXPECTATION OF PRIVACY

Level 2 and 3 AVs are not equipped to handle all of the driving features of the vehicle and drivers are advised by the automakers not to rely only on these technologies.[8] However, we have seen in the Tesla crash in 2016[9] and the Uber

---

5 For a broader investigation of the privacy implications of automated and connected vehicles (including external privacy interests and vehicle information systems) in Canada see Teresa Scassa, Jennifer A Chandler & Elizabeth F Judge, "Privacy by the Wayside: The New Information Superhighway, Data Privacy and the Deployment of Intelligent Transportation Systems" (2011) 74 Sask L Rev 87; Ian Kerr & Jason Millar, "Will Privacy Be the Next Moral Crumple Zone?" (2018) Report to Transport Canada [unpublished]; Philippa Lawson, "The Connected Car: Who Is in the Driver's Seat? — A study on privacy and onboard vehicle telematics technology" (2015) British Columbia Freedom of Information and Privacy Association, online: <fipa.bc.ca/wordpress/wp-content/uploads/2018/01/CC_report_lite.pdf>; Senate of Canada, Standing Senate Committee on Transport and Communications, *Driving Change — Technology and the Future of the Automated Vehicle* (January 2018) (Chair: David Tkachuk), online: <sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf>.

6 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11.

7 Disclosure of this data to the private sector is an equal and significant threat to the individual's privacy rights, but is not in the scope of this article.

crash in 2018[10] (and other small and non-lethal crashes) that technology enthusiasts tend to over-rely on the capabilities of these vehicles despite the warnings.[11] In order to shift the blame to the inattentive driver and avoid legal liability and media backlash, the carmakers now want to *see* what is going on inside the vehicle, through sensors and driver-facing cameras.[12] The manufacturers claim that this is a safety measure and that by making sure the driver is paying attention, the driver assistance systems will be able to operate as intended. However, the internal monitoring of vehicles creates a novel threat to individual privacy and has the potential to move from a safety feature to a widespread surveillance method, affecting the individual's *Charter* rights in a direct and substantial manner.

Section 8 of the *Charter*, which states that everyone has the right to be secure against unreasonable searches and seizures, protects the privacy of Canadians against intrusions of the state. The concept of reasonable expectation of privacy is the corner stone of a s. 8 analysis: if a reasonable expectation of privacy does not exist in a given situation, the search or seizure by the state will not violate the individual's s. 8 rights.[13] If it is established that the individual had a reasonable expectation of privacy in the particular circumstances, then the analysis proceeds to the second step, which is to determine whether the search or seizure conducted by the state was reasonable or not.[14] Therefore, as the first step to a *Charter* analysis, it is crucial to determine the existence of a reasonable expectation of privacy.

---

8 Tesla, "Model S Owner's Manual" (17 December 2018) at 80-94, online: <www.tesla.com/sites/default/files/model_s_owners_manual_north_america_en_us.pdf>.

9 Danny Yadron, "Tesla Driver Dies in First Fatal Crash While Using Autopilot Mode" *The Guardian* (1 July 2016), online: <www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk>.

10 Chaim Gartenberg, "Safety Driver of Fatal Self-Driving Uber Crash was Reportedly Watching Hulu at Time of Accident" *The Verge* (22 June 2018), online: <www.theverge.com/2018/6/22/17492320/safety-driver-self-driving-uber-crash-hulu-police-report>.

11 With misleading names such as "autopilot" and overly ambitious statements, carmakers are part to blame for the "automation bias" in drivers: Kerr & Millar, *supra* note 5 at 1.

12 Although many different tools are being developed, for relevance, I will focus on two technologies that are being widely used in today's AVs: driver sensors (Tesla) and facial recognition tools (Cadillac).

13 *R. v. Wise*, [1992] 1 S.C.R. 527, [1992] S.C.J. No. 16 (S.C.C.) at para. 4; *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, [1998] S.C.J. No. 83 (S.C.C.) at para. 31; *R. v. Tessling*, 2004 SCC 67, [2004] S.C.J. No. 63 (S.C.C.) at para. 18; *R. v. Evans*, [1996] 1 S.C.R. 8, [1996] S.C.J. No. 1 (S.C.C.) at para. 11; Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada*, Student Edition (Toronto: Thomson Reuters, 2018) at 2-14.

14 *R. v. Spencer,* 2014 SCC 43, 2014 CarswellSask 342, [2014] S.C.J. No. 43 at para. 68 ("A search will be reasonable if: (a) it was authorized by law; (b) the law itself was reasonable; and (c) the search was carried out in a reasonable manner") (S.C.C.) [*Spencer*].

A. The Current Approach to the Reasonable Expectation of Privacy of Drivers and Passengers

It has been accepted in Canadian jurisprudence that drivers have a reasonable expectation of privacy in their vehicles.[15] This expectation is not as high as one would enjoy in one's home due to the fact that driving is a regulated activity and needs monitoring for the public good.[16] Nevertheless, Canadian drivers' privacy in their automobiles is protected under the *Charter* from the prying eyes of the state.[17]

The expectation of privacy of non-owner drivers and passengers are not always that straightforward. In *Belnavis* the Supreme Court of Canada (SCC) addressed both of these issues. Regarding ownership, the SCC found that the driver, who was driving her boyfriend's car, had control of the vehicle and therefore had a reasonable expectation of privacy in it.[18] The SCC assessed the reasonable expectation of privacy of the passenger and emphasised that "whether a passenger will have a reasonable expectation of privacy in a vehicle will depend upon the totality of the circumstances".[19] Applying the test in *R. v. Edwards*,[20] the SCC took into consideration that even though the passenger was present at the time of the search, there was no evidence that she had any control over the vehicle or had any relationship with the driver which would establish some special access to the vehicle.[21] As a result, the SCC concluded that the passenger did not have a reasonable expectation of privacy.[22] However, the court also stated that a "privileged" passenger in the car, such as a spouse or someone with whom the driver was sharing responsibilities on a journey, might have a reasonable expectation of privacy.[23]

---

15 *R. v. Belnavis,* [1997] 3 S.C.R. 341, [1997] S.C.J. No. 81 (S.C.C.) [*Belnavis*] at para. 19; *Wise, supra* note 13 at para. 7; McIsaac, Shields & Klein, *supra* note 13 at 2-58.34.

16 *Belnavis, supra* note 15 at para. 39; *R. v. Harrison*, 2009 SCC 34, 2009 CarswellOnt 4108, [2009] S.C.J. No. 34 (S.C.C.) at para. 30; *R. v. Grunwald*, 2010 BCCA 288, 2010 CarswellBC 1392, [2010] B.C.J. No. 1088 (B.C. C.A.) at para. 36.

17 However, courts found that individuals who abandon their vehicle do not have a reasonable expectation of privacy: *R. v. Ellis*, 2013 ONSC 1494, [2013] O.J. No. 1274 (Ont. Sup. Ct. J.) at para. 102; *R. v. Cuff*, 2015 ONSC 6324, [2015] O.J. No. 5967 (Ont. Sup. Ct. J.) at para. 51.

18 *Belnavis, supra* note 15 at para. 19.

19 *Ibid* at para. 22.

20 [1996] 1 S.C.R. 128, 1996 CarswellOnt 1916, [1996] S.C.J. No. 11 (S.C.C.) at para 45.

21 *Belnavis, supra* note 15 at para. 22.

22 Taking the same approach, a Nova Scotia court also concluded that the passengers did not have a reasonable expectation of privacy stating that "there is no evidence that the two passengers exercised any control whatsoever over the vehicle or had an ability to exercise access or regulate access to the vehicle": *R. v. Curren,* 2003 NSPC 33, 2003 CarswellNS 293 (N.S. Prov. Ct.) at para. 16.

23 *Belnavis, supra* note 15 at para. 22. Using this analysis, an Ontario court found that the passengers in the vehicle had a reasonable expectation of privacy: "I have taken into

The courts have also addressed the reasonable expectation of privacy in commercial vehicles and have found that "the expectation of privacy in a commercial carrier is less than it is in a private automobile which in turn is less than it is in a residence".[24]

B. The Reasonable Expectation of Privacy in Level 2 and 3 AVs

The main technologies used for the internal surveillance of a semi-autonomous vehicle are sensors and cameras. Tesla uses a combination of hands-on-wheel torsion sensors with visual and audio alerts. Accordingly, it does not record any images of the interior,[25] but will record the driver's use of the steering wheel, his or her driving habits and whether he or she has obeyed the instructions of the system or not. The Cadillac Super Cruise (SC) has a more sophisticated internal tracking system. The SC uses a face-detection camera aimed at the driver and when the car detects that the driver's eyes are not on the road, the system starts giving warnings. If these warnings are ignored, the vehicle eventually comes to a controlled stop, as does a Tesla when its sensors' warnings are ignored. Cadillac claims that the SC does not record any footage but only makes sure that the driver pays attention.[26]

1. Charter Rights of the AV Driver

It has been established above that a driver has a reasonable expectation of privacy in the vehicle. Therefore, a search without proper lawful authority would be unconstitutional and would violate the driver's *Charter* rights. While an owner-driver always enjoys this right, a non-owner driver will need to demonstrate control over the vehicle. Will this outcome change in the case of access to the collected data from an AV?

Some technologies that are in use today offer us the chance to see the courts' interpretation about expectations of privacy in data collected by a vehicle. In *R.*

---

account that the accused appeared to be friends, and all of them were present when the vehicle was stopped and subsequently searched. In addition, each of them was to some extent in a position to admit or exclude others from entering the vehicle": *R. v. Emsley,* [2006] O.J. No. 5476, 2006 CarswellOnt 8821, 73 W.C.B. (2d) 536 (Ont. S C.J.) at para. 35. Also see: *R. v. Gauthier*, 1998 CarswellOnt 4636, 40 W.C.B. (2d) 283 (Ont. Ct. J. (Gen. Div.)) at paras 48-49.

[24] *R. v. Sadeghi,* 2007 SKQB 120, 2007 CarswellSask 197, 297 Sask.R. 96 (Sask. Q.B.) at para. 38; see also *R. v. Nolet,* 2010 SCC 24, 2010 CarswellSask 368, [2010] S.C.J. No. 24 (S.C.C.).

[25] Tesla added a driver-facing camera to the Model 3, which could potentially be used for driver monitoring purposes, but the device is currently not activated: Fred Lambert, "Tesla Chose Not to Add Eye-Tracking to Autopilot Because It's Ineffective, says Elon Musk" *Electrek* (14 May 2018), online: <electrek.co/2018/05/14/tesla-eye-tracking-autopilot-ineffective-elon-musk/>.

[26] Andrew J Hawkins, "Cadillac has a Secret Weapon in its Quest to Beat Tesla at Self-Driving" *The Verge* (15 April 2017), online: <www.theverge.com/2017/4/15/15289194/cadillac-super-cruise-lidar-map-interview-ny-auto-show>.

v. Hamilton,[27] an Ontario court had to decide whether the police violated the applicant's *Charter* rights after accessing the data held on his car's Airbag Control Module (ACM) which contained information regarding the vehicle's speed and braking in the seconds leading up to a fatal accident. The court concluded that the driver had a reasonable expectation of privacy in the data that was stored in the ACM and the warrantless access constituted a breach of his *Charter* rights. One year later, in *R. v. Glenfield*,[28] the contents of the applicant's vehicle's Event Data Recorder (EDR) were in issue and the court reiterated the ruling in *Hamilton* and decided that the warrantless access to the EDR data constituted a breach of the applicant's *Charter* rights.

The British Columbia Court of Appeal (BCCA) came to a different conclusion in *R. v. Fedan*.[29] In this case, the court found that the appellant did not have an objectively reasonable expectation of privacy in the car's sensing diagnostic module (SDM)[30] because the SDM did not provide any data with personal identifiers.[31] The court also stated that the information regarding the last five seconds before the crash was not private as the activity was in public and witnesses had given statements regarding the erratic driving of the appellant.[32]

The verdict in *Fedan* is significant and important to analyze in the context of AVs. The court stated that the SDM "did not capture any information that revealed intimate details of Mr. Fedan's biographical core, and in particular about who was driving the car. Further evidence had to be obtained to connect the driving of his vehicle to Mr. Fedan himself".[33]

How would the courts evaluate the data extracted from Tesla's wheel torque sensor or Cadillac's face detection cameras? It can be expected that the courts in *Hamilton* and *Glenfield* would accept that the drivers' reasonable expectation of privacy exists in the data produced by these systems. The B.C. Court in *Fedan* might disagree; Tesla's sensor or Cadillac's camera do not record the person *per se*, but keep a log of their actions. The court could reiterate its position and state that these systems do not capture any personal information. However, stating that the SDM's data does not include any personal information is not an accurate assessment: the system records the driver's interactions with the car, which is information about the driver, not the car.[34] Furthermore, even if the

---

[27] 2014 ONSC 447, 2014 CarswellOnt 1873, [2014] O.J. No. 747 (Ont. S.C.) [*Hamilton*].

[28] 2015 ONSC 1304, 2015 CarswellOnt 3290, [2015] O.J. No. 1212 (Ont. S.C.) [*Glenfield*].

[29] 2016 BCCA 26, 2016 CarswellBC 112, [2016] B.C.J. No. 91 (B.C. C.A.) [*Fedan*].

[30] SDM has the same functions with the EDR and ACM systems mentioned. These systems are for the deployment of airbags but also record information about the car in the last few seconds before a crash.

[31] A Quebec court took the same approach and decided that the driver didn't have a reasonable expectation of privacy on the airbag system data as it didn't reveal any personal information: *R. c. Gauthier,* [2003] J.Q. no 7370, J.E. 2003-1473 (C. Q.).

[32] *Fedan, supra* note 29 at para. 84.

[33] *Ibid* at para. 81.

[34] Teresa Scassa, "The Reasonable Expectation of Privacy and Your Car's Airbag System"

court's position on SDMs were to be accepted, it must be noted that there is a significant distinction between SDM's data and the data collected via the new technologies in AVs. The SDM reveals very limited technical information only for the last five seconds before a crash, whereas a sensor or camera system will continuously record data and keep logs on the driver's choices and behaviour. Therefore, even in the early stages of these technologies, where actual footage is not yet being recorded, an unauthorized access to these logs and records will violate the driver's informational privacy and trigger the his or her *Charter* rights.

Although carmakers claim that no identifiable information is collected and nothing is recorded at the current technology level of sensors and cameras, the collection of data will continue to increase as these systems become more familiar to users.[35] As internal monitoring increases and gets even more "personal", the BCCA's misinterpretation of the collected data and the verdict in *Fedan* will be irrelevant. In any case, no matter what type of information is received from the AVs – whether it contains logs of sensor movements or actual footage of the interior – the driver has a reasonable expectation of privacy.[36]

2. *Charter Rights of the AV's Non-owner Driver and Passenger*

The SCC found in *Belnavis* that non-owner drivers who are driving the car with permission of the owner and are in a position to exhibit control over the car have a reasonable expectation of privacy in it and are secure against physical searches.[37] In *Glenfield*, the informational privacy of the non-owner driver was protected and the fact that the he was not the owner of the vehicle did not affect

---

Teresa Scassa (blog) (3 November 2014), online: < www.teresascassa.ca/index.php?option = com_k2&view = item&id = 172:thereasonable-expectation-of-privacy-and-your-cars-airbag-system&Itemid = 80 > .

[35] The German "Intelligent Car Interior" project: "We are expanding sensor technology to the entire interior . . . Using depth-perception cameras, we capture the vehicle's interior, identify the number of people, their size and their posture. From this we can deduce their activities." Fraunhofer, "Camera-based Technology Tracks People in Car Interiors" (1 August 2016), online: < www.fraunhofer.de/en/press/research-news/2016/august/camera-based-technology-tracks-people-in-car-interiors.html > [*Fraunhofer*].

[36] It must be noted that establishing a reasonable expectation of privacy does not necessarily mean that this data cannot be obtained by the state. Government organizations can acquire personal information in which the individual has a reasonable expectation of privacy through judicial and lawful processes, such as a production order. In such a situation, even though the individual has a reasonable expectation of privacy, the disclosure of information to state will not be in violation of his or her *Charter* rights. Accordingly, the goal of this article is not to claim that this data will never be procured by the state, rather is to claim that the state cannot obtain this data at will, without going through the necessary judicial processes that essentially provide a screening mechanism. Therefore, considering that any incident regarding the AV might justify reasonable grounds for such a court order, the effectiveness of the screening mechanism, which is not in the scope of this paper, will be as important in protecting individuals' privacy.

[37] *Belnavis, supra* note 15 at para. 19.

his expectation of privacy as he demonstrated control over the vehicle.[38] Therefore, it can be concluded that a non-owner driver will have a reasonable expectation of privacy in the data that has been collected by the AV as long as he or she has the consent of the owner to operate the vehicle and has demonstrated control over it.

At the current state of the technology the sensors and cameras are not yet capturing passengers. Therefore, the territorial privacy approach established in *Belnavis*, which has since been consistently adopted by courts in subsequent case law, will still be valid for the current AVs.[39] This does not mean that a passenger can *never* have a privacy interest within a vehicle. Courts found that passengers may have a reasonable expectation of privacy in their specific belongings within a car[40] and in cases where they were asked for identification without reasonable grounds.[41] However, in the context of AVs, since the current internal surveillance practices that are examined in this paper are not aimed at the passengers, the determinative factor will be the passengers' ability to establish a reasonable expectation of privacy concerning the vehicle itself and their ability to challenge the search of the vehicle. Therefore, in the current state of the technology, the passenger would need to demonstrate control or a "privileged access" to the vehicle, as determined by *Belnavis*. This conclusion will change when the current means of internal surveillance develop to a point where it exceeds the driver and the entire interior of the AVs are recorded. As a result of this surveillance, the informational privacy of the passengers will emerge, changing the conception of the reasonable expectation of privacy of a passenger. In this case, the passenger

---

[38] *Glenfield, supra* note 28.

[39] In a recent case, *R. v. Steele*, 2015 ONCA 169, [2015] O.J. No. 1253 (Ont. C.A.) at para. 20, the Ontario Court of Appeal decided that a passenger, who was in a vehicle owned by his mother, did not have a reasonable expectation of privacy in the vehicle. In reaching this conclusion, the ONCA cited *Belnavis* and determined that even though the car belonged to a family member, the appellant did not identify himself as the person to whom the car had been loaned and as a result did not demonstrate control over it: "[h]e was only a passenger in a vehicle driven by another person who claimed to have borrowed the car . . . the driver was attempting to produce required documentation to police, and had apparent control of the vehicle." See also *R. v. Belcourt,* 2012 BCSC 229, [2012] B.C.J. No. 2632 at para. 9; *R. v. Boudreau,* 2006 BCSC 914, [2016] B.C.J. No. 1534 (B.C. S.C.) at paras 54-55.

[40] Although passengers will not have a reasonable expectation of privacy in the vehicle and cannot challenge the search of the vehicle, they may have a reasonable expectation of privacy on their specific belongings within the vehicle. In *R. v. Gregoire*, 2005 ABQB 340, [2005] A.J. No. 529 (Alta. Q.B.) at para. 341, the court cited *Belnavis* to determine that the accused did not have a reasonable expectation of privacy in the vehicle, however decided that she had a reasonable expectation of privacy in her belongings and could challenge the search of her belongings.

[41] Courts have accepted that the request by an officer for a passenger's identification, where such a request was not consistent with the reason that the vehicle was stopped by the officer, would constitute a breach of the passenger's s. 8 rights: see *R. v. Mhlongo*, 2017 ONCA 562, [2017] O.J. No. 3439 (Ont. C.A.) at para. 51; *R. v. Harris*, 2007 ONCA 574, [2007] O.J. No. 3185 (Ont. C.A.) at para. 44.

would not need to establish control or a privileged access to the vehicle on contrary to the territorial privacy approach in *Belnavis*. The goal of the industry is gathering as much information as possible from the interior of the vehicle and the interest in monitoring everyone in the vehicle has already been declared.[42] Considering the rapid developments in the field, it might not be long before passenger behaviour is monitored and when it does, the courts will need to develop a new understanding regarding the reasonable expectation of privacy of passengers.

C. Constitutionality of Disclosure to the State under *PIPEDA* and Consent

1. Disclosure of personal information in accordance with PIPEDA

The *Personal Information Protection and Electronic Documents Act (PIPEDA)*[43] governs the collection, use and disclosure of personal information in the private sector and would apply to the relationship between the customer and the party he or she purchases or leases the AV.[44] Section 7(3)(c.1)(ii) of *PIPEDA* allows businesses to disclose personal information to government institutions that identify a lawful authority to request the information for the purpose of enforcing laws in Canada. Accordingly, can businesses disclose information obtained from the vehicle sensors to law enforcement agencies in case of a crash or any other criminal offence?

In some cases, courts have interpreted this section of *PIPEDA* as an authorised circumvention to the requirement of a court order, meaning that state officials could access the data in the hands of private organisations simply by requesting for the purposes of law enforcement.[45] In *R. v. Ward,*[46] the Ontario Court of Appeal (ONCA) examined the validity of a disclosure made pursuant to *PIPEDA*'s s. 7(3)(c.1)(ii). In this case, the internet service provider (ISP)

---

42 *Fraunhofer, supra* note 35.

43 *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5 [*PIPEDA*].

44 Except in British Columbia, Alberta and Quebec, which have their own private sector privacy legislations that have been declared substantially similar to *PIPEDA* in accordance with s. 26 (2)(b) of the Act.

45 *R. v. Brousseau,* 2010 ONSC 6753, 2010 CarswellOnt 10252, [2010] O.J. No. 5793 (Ont. S.C.J.) at para. 42; *R. v. McNeice*, 2010 BCSC 1544, [2010] B.C.J. No. 2131 (B.C. S.C.) at para. 43. Another case of relevance *R. v. Gomboc,* 2010 SCC 55, [2010] S.C.J. No. 55 (S.C.C.) [*Gomboc*]. In this case, the question in front of the SCC was whether the unauthorized access to the accused's electric consumption data violated his *Charter* rights. The majority found that the accused did not have a reasonable expectation of privacy on the consumption data. One of the factors that the majority took into consideration in reaching this conclusion was the fact that the *Code of Conduct Regulation* (Alta. Reg. 160/2003, s. 10(3)(f)), which was applicable to the relationship between the accused and the electric company, allowed disclosure to officers who request it for investigation purposes unless the customer explicitly requests otherwise.

46 2012 ONCA 660, 112 O.R. (3d) 321, 296 O.A.C. 298 (Ont. C.A.) [*Ward*].

disclosed the internet protocol (IP) address of the accused to law enforcement in cooperation with an ongoing child pornography case. The ONCA found that "*PIPEDA* does not create any police search or seizure powers" and that a court order was required for such a disclosure.[47] However, considering the grave nature of the crime and the legitimate interest of the ISP in the disclosure, the court concluded that the accused did not have a reasonable expectation of privacy.[48]

In *Spencer*,[49] similar to *Ward*, the subject matter in front of the SCC was regarding the unauthorized disclosure of the accused's IP address by the ISP to law enforcement in course of a child pornography investigation. The SCC agreed with the ONCA that *PIPEDA* did not create any police search powers but came to a different conclusion.[50] The court found that although the considerations of ONCA in *Ward* are relevant they "cannot override the clear statutory language of s. 7(3)(c.1)(ii) of PIPEDA, which permits disclosure only if a request is made by a government institution with 'lawful authority' to request the disclosure".[51] Establishing that the accused had a reasonable expectation of privacy on the data, the court emphasized that "it would be reasonable for an Internet user to expect that a simple request by police would not trigger an obligation to disclose personal information or defeat *PIPEDA*'s general prohibition on the disclosure of personal information without consent."[52] Therefore, it has been established by the SCC in *Spencer* that s. 7(3)(c.1)(ii) of *PIPEDA* cannot be accepted as a source for lawful authority that would override the requirement of a production order. Accordingly, businesses cannot disclose the data collected within the AVs to state officials relying on s. 7(3)(c.1)(ii) of *PIPEDA*.

2. Does the consent of the owner affect his or her Charter rights?

If the owner of the AV, as part of the sale or rental agreement, gives his or her consent to the carmaker or dealer for the disclosure of personal information to law enforcement agencies, how would the individual's *Charter* right to be secure from unreasonable searches be affected?

The consumer contracts of large companies are almost always one-sided and not negotiated with the consumer. Instead, the customer gives consent by signing a non-negotiable agreement or accepting the terms and conditions of that company. There is a clear inequality in bargaining powers between the consumer and the carmaker or dealer of the AV. Therefore, can it be said that the consumer is making a conscious and voluntary choice to waive his or her *Charter* right to be free from unreasonable searches?

---

47 *Ibid* at para. 46.

48 *Ibid* at paras. 98-107.

49 *Spencer, supra* note 14.

50 *Ibid* at para. 71.

51 *Ibid* at para. 63.

52 *Ibid* at para. 62.

In *R. v. Wills,*[53] the ONCA determined that in order for an individual to have consented to what would otherwise be an unauthorized search, the consent must be given voluntarily (either implied or express) by a person who is authorized to give such consent and is aware of the nature and the consequences of the consent and the waived right.[54] Even though this criterion was established by the ONCA and was later adopted by the SCC,[55] it was not applied in *Gomboc* or *Ward*. In *Gomboc*, although it was clear that the accused did not know or understand that he could have opted-out from the provision that enabled the third party to disclose information to the state, the fact that he did not opt-out was considered to be a factor in determining the reasonable expectation of privacy. However, while noting that the accused had the power to opt-out, the majority pointed out that one should act cautiously when dealing with contracts of adhesion.[56] The ONCA in *Ward* considered the user policy agreement of the ISP, which notified the customer that their data would be disclosed to law enforcement agencies, to be a relevant factor in the evaluation of the totality of the circumstances.[57]

In *Spencer*, the SCC considered user policies of the ISP and came to a different conclusion. The court found that the three documents governing the relationship between the accused and the ISP were "confusing and equivocal in terms of their impact on a user's reasonable expectation of privacy in relation to police-initiated requests for subscriber information." As the contractual terms pointed to *PIPEDA*, the court turned its attention to the legislation, ultimately deciding that the regulation does not allow access without lawful authority.[58]

The SCC did not clearly define the validity of consent given in unilateral agreements that undermine *Charter* rights in *Spencer*.[59] However, in a more recent case, *Douez v. Facebook*,[60] the SCC examined the online contract between a consumer and Facebook to examine the validity of a jurisdictional clause that the consumer accepted as part of the terms and conditions of subscribing to Facebook's services. The court found that the contractual term was unenforceable due to the fact that there was a "gross inequality of bargaining power" between the parties and the importance of the "quasi-constitutional privacy rights" that were at stake.[61]

---

53 *R. v. Wills*, [1992] O.J. No. 294, 12 C.R. (4th) 58, 15 W.C.B. (2d) 415 (Ont. C.A.) [*Wills*].

54 *Ibid* at para. 69.

55 *R. v. Borden*, [1994] 3 S.C.R. 145, [1994] S.C.J. No. 82, 119 D.L.R. (4th) 74 (S.C.C.) at para. 34.

56 *Gomboc, supra* note 45 at para. 33.

57 *Ward, supra* note 46 at para. 107.

58 *Spencer, supra* note 14 at para. 63.

59 Mark MacAulay, "Contracts, Legislative Frameworks and the Reasonable Expectation of Privacy: Rethinking Section 8 in the Service Provision Context" (2015) 20 Can Crim L Rev 111 at 113.

60 2017 SCC 33, [2017] S.C.J. No. 33, 411 D.L.R. (4th) 434 (S.C.C.) [*Douez*].

61 *Ibid* at para. 76.

The SCC's rulings in *Spencer* and *Douez* would suggest that consent given by the consumer within the terms and conditions for the sale or lease of the AV, enabling the business to disclose personal information to state officials will not be accepted as well. Although this point is not clearly indicated in *Spencer*, in *Douez* the court clearly rejected the waiver of constitutional rights in unilateral contracts where there is no meaningful consent. Similar to *Douez,* the consumers of AVs are in a position where certain provisions are forced upon them by a stronger party as a condition of having access to the service and the disclosure of this data to law enforcement agencies pose a great threat for the person's privacy and threatens the individual's *Charter* rights.

It can be argued that the purchase of an AV is non-essential and that the customer has the chance to buy another car if he or she doesn't want to agree to the terms and conditions. The SCC answered a similar argument in *Douez* about the complainant's chance to use another social media platform or avoid using any platform. The court dismissed this argument by stressing the importance of social media and opined that the chance to stay "offline" is not possible in today's connected world.[62] In the AV context, this argument might not be accepted as the driver assisting features of the AVs today can be seen as a luxury rather than a necessity. However, the reality is that many of the new vehicles on the market today have certain features that collect personal information which may endanger the privacy of their users. Also, even though full automation will not be available for customers anytime soon, the development and use of semi-autonomous vehicles is increasing every day and in the near future the classic car will start to disappear and automated vehicles will become widespread and perhaps the only choice.

It is also worth noting that when the internal surveillance in AVs start capturing more than the driver, even if the driver gives a valid and explicit consent for the disclosure of the data collected by the AV, this consent will not have an effect on third parties, such as passengers. The SCC has determined that third-party consent is invalid and in such a situation, driver's consent will only have an effect on his or her reasonable expectation of privacy.[63]

III. CONCLUSION

The introduction of internal surveillance methods in semi-autonomous vehicles produces a novel privacy threat to society. As the technology becomes more familiar and widely used, the collection of data will increase and the privacy of a traditionally private space will be seriously compromised.

One of the significant effects of AVs on society is the threat they pose to an individual's *Charter* right of being free from unreasonable searches. The current

---

62 *Ibid* at para. 56.

63 *R. v. Cole,* 2012 SCC 53, [2012] S.C.J. No. 53, 353 D.L.R.(4th) 447 (S.C.C.) at paras. 78-79; *R. v. Reeves*, 2018 SCC 56, [2018] S.C.J. No. 56, 427 D.L.R. (4th) 579 (S.C.C.) at paras 50-52.

jurisprudence in Canada that has been evaluated in this article demonstrates that the introduction of AVs will not have an immediate negative affect on the individuals' *Charter* rights, at least at the current stage of the technology.

The drivers will continue to have a reasonable expectation of privacy that will restrain the state from prying into their collected data without any lawful authority. The passengers of private or commercial AVs who are unable to prove a special access to the car will not have a reasonable expectation of privacy and thus a *Charter* protection on their collected data. Although the current level of surveillance tools that were examined in this paper do not pose a direct threat towards passengers yet, this will quickly change and if courts cannot adjust their current evaluation of passengers' privacy in vehicles, severe privacy violations will be inevitable in the near future.