Privacy Under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles*

Chelsey Colbert

March 16, 2018

The Autonomous Vehicles are already here;
they're just not very evenly distributed.[1]

Connected vehicles ("CVs") and Autonomous Vehicles ("AVs") pose novel ethical and legal challenges that industry and governments must immediately address, particularly about privacy and data protection. There is a sense of urgency behind deploying connected and automated vehicles: all major commercial automakers, as well as universities and technology companies like Google, Apple, and Uber, are involved in research and development of connected and autonomous vehicle technology.[2]

True autonomous capabilities are expected to be available to consumers within five to 20 years[3] and while this may signal to some that we have a bit of breathing room to develop regulatory frameworks, our feet need to stay firmly on the gas pedal for several reasons. First, semi-autonomous vehicles are already on the market and industry is racing to deploy truly driverless vehicles. Waymo announced that it not only intends to deploy driverless cars, but these cars will operate in its own ride-hailing business.[4]

---

*This paper represents the views solely of the author and is not intended as legal advice. Many thanks to Suzie Dunn (@suziemdunn) for her comments and support throughout writing this paper.

[1] "The future is already here — it's just not very evenly distributed." - William Gibson.

[2] See for example, Center for Automotive Research at Stanford, online: < https://cars.stanford.edu/>.

[3] This is a broad estimate. Some experts predict in 10 to 15 years, see Senate of Canada, "Driving Change: Technology and the future of the automated vehicle", Report of the Standing Senate Committee on Transport and Communications, January 2018, p 9, online: <https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf> [Senate, Driving Change]. Other predict a much shorter timeline. In October 2017, there were 42 companies testing almost 300 self-driving vehicles in California, see Andrew J Hawkins, "Autonomous cars without human drivers will be allowed on California roads starting next year", The Verge (11 Oct 2017), online: < https://www.theverge.com/2017/10/11/16458850/self-driving-car-california-dmv-regulations>. Google's Waymo tested autonomous vehicles without a safety driver in the fall of 2017. Andrew J Hawkins, "Waymo is first to put fully self-driving cars on US roads without a safety driver", The Verge (7 November 2017), online: <https://www.theverge.com/2017/11/7/16615290/waymo-self-driving-safety-driver-chandler-autonomous>.

[4] Waymo has been testing approximately 600 autonomous vehicles in the Phoenix area since April 2017 and launched an "Early Rider Program" for residents to test the vehicles and provide feedback. See https://waymo.com/. Jack Stewart, "Google's Finally Offering Rides In Its Self-Driving Minivans", Wired

Second, we should not underestimate the disruptive impact the ride-sharing and mobility-as-as-service ("MaaS") industry will have on consumer adoption of AVs and on data privacy laws. Many people will first experience an AV through a ride-sharing service, rather than purchasing their own AV. Third, autonomous capabilities depend on connectivity and thus all autonomous vehicles will also be connected vehicles, which are already mainstream.

Governments are reluctant to slow down innovation with red tape since, by one estimate, the economic benefit of AVs could reach an estimated CAD$65 billion annually in accident avoidance, heightened productivity, improved fuel economy[5] and congestion avoidance.[6] There are other benefits to society, for example, since once vehicles no longer require a human in control, previously immobile groups of people will experience an increase in mobility and independence.[7] However, a good portion of the population in North America will not own an AV for at least three reasons. First, AVs will be too expensive for most to own.[8] Second, there is a trend of less vehicle ownership, particularly in urban areas and among young people.[9] Third, AVs will be better suited to, and more widely available in, some environments over others.[10]

(25 April 2017), online: <https://www.wired.com/2017/04/googles-finally-offering-rides-self-driving-minivans/>. Alison Griswold, "Waymo is readying a ride-hailing service that could directly compete with Uber", Quartz (16 February 2018), online: <https://qz.com/1208897/alphabets-waymo-googl-is-readying-a-ride-hailing-service-in-arizona-that-could-directly-compete-with-uber/>.

[5] This point has been debated. On one hand, there may be more empty cars on the road or cars with just one passenger. On the other hand, platooning vehicles, with vehicles driving very close to each other, provides many benefits including improved fuel economy, higher speeds of travel and fewer crashes. See Jed Chong, Library Of Parliament Research Publications, "Automated and Connected Vehicles: Status of the Technology and Key Policy Issues for Canadian Governments", (29 September 2016), online: < https://lop.parl.ca/Content/LOP/ResearchPublications/2016-98-e.html#ftn29>; U.S. Department of Energy, National Renewable Energy Laboratory, "Truck Platooning Testing," *Transportation Research*; and Government of the Netherlands, "Truck Platooning," *Mobility, public transport and road safety*.

[6] The Conference Board of Canada, "Automated Vehicles. The Coming of the Next Disruptive Technology", January 2015, p 20, online: < http://www.cavcoe.com/articles/AV_rpt_2015-01.pdf>. Senate, Driving Change, at 10.

[7] RAND, Autonomous Vehicle Technology: A Guide for Policymakers, 2016, at xv [Rand, Guide for Policymakers].

[8] When they first hit the market at least. The cost for an autonomous vehicle is around $250,000. Even if autonomous capabilities were to come down in price, adding $10-15,000 to a car that already costs $25,000 is prohibitively expensive for the average person. Steve LeVine, "What it really costs to turn a car into a self-driving vehicle", Quartz (5 March 2017), online: <https://qz.com/924212/what-it-really-costs-to-turn-a-car-into-a-self-driving-vehicle/>.

[9] KPMG, "Global Automotive Executive Survey 2017", at 25, online: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/01/global-automotive-executive-survey-2017.pdf> [KPMG, Survey]. Currently, however vehicles are a staple of many people's lives. Going without

Connected vehicles are already on the market and are gaining in popularity: in the first quarter of 2016, connected vehicles accounted for a third of all new cellular devices.[11] Even an older vehicle can be modified to become a CV by plugging a dongle into a port in the vehicle.[12] The challenges that have arisen from CVs, such as legal and ethical uses of customer data, serve as a prediction for some of the issues that will also arise with AVs, but there will also be new and unanticipated challenges. These challenges can ultimately help legislators and industry prepare for when fully autonomous vehicles - in a fully connected city - do become reality.[13]

This paper takes a prospective policy approach to the data privacy challenges of connected and autonomous vehicles. It seeks to provide insight and direction to policy-makers and industry by canvassing what sets AVs apart from current technology, such as mobile phones, and it looks at laws and policy approaches in three jurisdictions to highlight some areas of tension for consumer data privacy protection.

To **begin**, this paper demonstrates that connected and autonomous vehicles, while at first glance may seem no different than the mobile phones that are always on our bodies,

---

a vehicle is not an option for many Canadians, since many rural, and even urban, areas are easier to navigate with vehicles; transit or ride-sharing is just not a convenient option. 80% of Canadian households own at least one vehicle. Philippa Lawson, Brenda McPhail and Eric Lawson, "The Connected Car: Who is in the Driver's Seat? – A study on privacy and onboard vehicle telematics technology, BC FIPA (with help from the Canadian Internet Policy and Public Interest Clinic], Vancouver, 2015, at 8 [Lawson, The Connected Car].

[10] Compare the clean and well-marked roads of Palo Alto in December with the snowy, icy roads of Ottawa in December.

[11] In 2016, AT&T, for example, had eight million cars on its network. Kristen Hall-Geisler, "More cars than phones were connected to cell service in Q1", TechCrunch (20 June 2016), online: < https://techcrunch.com/2016/06/20/more-cars-than-phones-were-connected-to-cell-service-in-q1/>.

[12] Car connectivity will soon become standard in all new vehicles. In 2016, AT&T had eight million connected cars on its network. See Kumar Abhimanyu, "How connected cars are turning into revenue-generating machines", (28 August 2016) TechCrunch, online: <https://techcrunch.com/2016/08/28/how-connected-cars-are-turning-into-revenue-generating-machines/>. Nissan will begin equipping vehicles with its connected system in 2018 and it will be used in 90% of the vehicles built by Nissan, Renault, and Mitsubishi. See Lindsay Chappell, "Renault-Nissan connected-car program is a big win for Continental", (3 November 2017) Automotive News Europe, online: < http://europe.autonews.com/article/20171103/COPY/311039996/renault-nissan-connected-car-program-is-a-big-win-for-continental>. Even a 2010 Toyota Land Cruiser can become a Wi-Fi hotspot by plugging a dongle into the car's OBD-II port. See AT&T, Connected Car Solution, online: <https://www.att.com/shop/wireless/connected-car/do-it-yourself.html?vehicleid=226951&header=&sessionID=B559EE60-36C1-444A-9163-B3276B706786#Close>.

[13] "Revenues in the connected car market will nearly quadruple between 2015 and 2020, led by driver assistance and safety technologies", PwC, "In the Fast Lane: The Bright Future of Connected Cars", 2014,

actually present data privacy challenges unlike other technology. The **next** section focuses on one of the many emerging challenges to data privacy: the upcoming battle for data ownership and obtaining valid consumer consent,[14] and suggests one possible solution. It also illustrates that good data privacy and data management policies are beneficial to consumer and industry. The **third** section provides a high-level overview of the current regulatory and policy landscapes in Canada, the United States, and the European Union. The **fourth** section will highlight some of the major trends and factors pushing towards internationally harmonized and sector-specific laws. The paper **concludes** that an international data privacy framework should be developed and by addressing the short-term challenges of connected vehicles, while allowing experimentation of advanced technology like AVs, we can be better prepared for the day AVs are mainstream.

I. Connected Vehicles Are More Than Mere Extensions of Mobile Devices

In terms of both quality and quantity, the data collected and generated from connected and autonomous vehicles goes beyond the breadth and depth of what our current mobile devices collect.[15] The data collected by these vehicles includes health data, driver behaviour, location data, personal contacts, and personal schedules and personal preferences and habits can be inferred from this data. Indeed, a driver's mobile phone is encouraged to become *part* of the connected vehicle ecosystem.[16]

Car manufacturers no longer only produce and sell vehicles – the hardware - they are also the companies that produce the software. Connected and autonomous vehicles will

[14] Data sovereignty, data localization laws, and transborder data flows are another set of data privacy challenges with compliance costs.
[15] Lawson, The Connected Car at 5.
[16] Our need to be constantly "connected" has been documented many times. For example, "[n]early a quarter of teenagers, according to a Pew Research Center study, self-report going online "almost constantly," and a Department of Health and Human Services report from 2013 shows adolescents spend almost eight hours a day consuming media, from videos to picture-posting to emailing." Sanjena Sathian, "Special Series: What If Designers Took A Hippocratic Oath?", OZY (5 Jan 2016), online: < http://www.ozy.com/fast-forward/special-series-what-if-designers-took-a-hippocratic-oath/64873>. See also, Mireille Hildebrandt's "onli*f*e world", where 'real' life is neither on- nor offline. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Cheltenham: UK, Edward Elgar Publishing, 2015.

collect and generate data about the driver and passengers and share it in real time with the vehicle's manufacturer. This creates a communication portal between the manufacturer and the vehicle and the individual(s) inside the vehicle. This new reality is turning vehicle purchase agreements into privacy policies, which is something consumers are likely not primed to expect when purchasing or renting a vehicle,[17] especially when the vehicle does not look any different than its analogue cousin.[18]

One of the most pressing challenges for policy-makers regarding autonomous vehicles is whether current data privacy laws are robust enough to withstand the privacy and data security challenges that AVs will bring.[19] Consider that if your connected vehicle detects that your blood pressure is elevated it can switch to soothing music on your commute to work. Then, on your way home, your vehicle can make a restaurant reservation at a certain time based on your food preferences, traffic conditions, and previous driving behaviour.[20] The data being collected and shared in these scenarios, and the subsequent decisions being made about us based on this data, adds complications not present with our current mobile devices.

Those developing connected and autonomous vehicles will have direct access to various types of consumer data, such as account information, vehicle diagnostics data, driver behaviour, location data, and biometric and heath data about the consumer.[21] The primary purpose for collection is to allow the connected and autonomous features to function, however there are secondary and tertiary uses, like targeted marketing, to

---

[17] See for example, Peter Holley, "Big Brother on wheels: Why your car company may know more about you than your spouse.", (15 January 2018), The Washington Post, online: < https://www.washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse>.

[18] Until autonomous vehicles are mainstream, manufacturers may try to conceal the parts of the vehicle that make it connected and autonomous since there is the view that consumers do not want their vehicles to look any different than they currently do. There may be other reasons to conceal that a vehicle is in fact an AV. See Dom Galeon, "People Are Reportedly Attacking Driverless Cars in California", Futurism (7 March 2018), online: < https://futurism.com/people-attacking-driverless-cars-california/>.

[19] Telematics and infotainment systems in CCs and AVs generate data which reveal personal lifestyle and behavioural preferences. The data generated include individual and vehicle performance data, driver behaviour, biometrics and health data, location data, the driver's personal communications, personal contact list and schedules, as well as other entertainment and consumption data. See Lawson, The Connected Car.

[20] *Ibid* at 44.

[21] *Ibid* at 70.

prevent and detect fraud, and for research and internal business purposes. The personal data collected and generated by the vehicle will be extremely valuable to manufacturers[22] as well as to vehicle rental companies, car sharing, and mobility-as-a-service ("MaaS") companies for marketing and product development. Primary and secondary uses of data will also provide benefits to the consumer.

Connected vehicles will increasingly collect, use and share personal information about the driver and this raises legal privacy issues that industry must be conscious of, such as whether there are data localization laws or whether the organization has valid consent to collect, share and sell the individual's personal information for all purposes. Furthermore, the data, the individuals, and the vehicles will cross borders, sometimes contemporaneously. Because data privacy laws differ depending on the jurisdiction, this brings up interesting compliance and enforcement issues for organizations, as well as challenges for policy-makers drafting domestic regulations while being mindful of international laws and the impact regulations will have on business development. Connected and autonomous vehicles will also collect and generate data that is not "personal information"[23], such as speed of the vehicle or other vehicle diagnostics and aggregate traffic information, yet this will still raise controversial questions without clear answers.[24] Regardless of whether the data is considered "personal information", it is essential that these challenges be examined *before* AVs become a part of mainstream transportation in a connected city.

The data available to connected and autonomous vehicles also pushes the challenges past data privacy laws. Therefore, the solutions should also be a mix of data privacy regulations, industry standards, codes of practice, competition law, and savvy private

[22] *Ibid* at 70.
[23] As defined by data privacy legislation and jurisprudence, which can and does differ by jurisdiction.
[24] We see this debate in the smart city context. Organizations that are partnering with cities, and contracting with entities incorporated by cities, stand to benefit from both personal information of consumers and from the environmental and city data. This latter category of data are things like traffic patterns, air quality, trash sensors, etc. This data is not personal information and is not protected under privacy legislation, yet is extremely valuable to organizations for future business models and for cities. Because this data is not governed under privacy laws, the ownership will be a matter of negotiation and the subject of contracts. See Sidewalk Labs in Toronto, Canada, online: https://sidewalktoronto.ca/. See this video for a discussion on the proposed smart city in Toronto: "Building Smarter Cities", The Agenda with Steve Paikin, (13 November 2017), online: < https://tvo.org/video/programs/the-agenda-with-steve-paikin/building-smarter-cities>.

contracts. An international data privacy framework for connected and autonomous vehicles is needed. The ideal framework would protect the privacy interests of individuals, is flexible enough to adapt to technological advances in transportation, yet allows industry and individuals to take advantage of AI and data analytics for economic and social gain.

There are two main elements of connected and autonomous vehicles that set it apart from current technology and underlie much of the discussion below. First, connected and autonomous vehicles will be comprised of technology that make AVs the pinnacle of the Internet of Things ("IoT").[25] Second, the trend of ride-sharing and MaaS should not be overlooked when addressing data privacy policy and compliance challenges.

The Technology

Consumers increasingly expect their vehicles to be connected and many consumers are interested in autonomous capabilities. Consumers want their vehicles, laptops, and smartphones to be synced and for their vehicles to read off incoming texts or to assist them with navigation to destinations, such as specific retail outlets.[26] Our vehicles are quickly becoming an extension of our homes and offices,[27] and as more connected and autonomous capabilities become available, vehicles will be akin to personal assistants in helping to accomplish personal or work commitments.

Connected car technology can be broken into two broad categories[28]: infotainment and telematics.[29] Telematics is the technology that collects and sends data from the vehicle in real time, allows the vehicle to provide enhanced safety features, and enables

[25] Lawson, The Connected Car at 13.
[26] Rand, Guide for Policymakers at 82-83.
[27] Lawson, The Connected Car at 8.
[28] For an in depth discussion of connected vehicle technology and its applications, see chapters 2-5 of Lawson, The Connected Car.
[29] To operate safely and effectively, vehicles will need to communicate with other vehicles via the vehicle-to-vehicle (V2V) and city infrastructure via vehicle-to-infrastructure (V2I) communications. This type of communication could also add a level of redundancy in case the vehicle's sensors fail, allowing the vehicle to rely on the sensors of nearby vehicles.

autonomous capabilities.[30] To ensure the vehicles remain as secure as possible and to push software upgrades, the vehicles will need to communicate with its manufacturer or with other third parties. Autonomous vehicles will also have this technology, yet AVs will also be in control of where and how the vehicle travels. The data collected and generated in an AV will be used to develop the neural networks that will allow the vehicles to operate more efficiently, analyze accidents, and understand traffic flow.[31] Infotainment systems in the vehicle, which offer information, like navigation, or entertainment, like music, is a perk for those in the vehicle and will be promoted to increase consumer adoption of connected capabilities.[32] The data generated by connected and autonomous vehicles will also be used to create detailed profiles of consumers for marketing and predicting behaviour.[33] Thus, we can see that there are many layers of data collection and use, some for primary purposes, like vehicle safety, and other collection is for non-essential purposes, like third-party marketing.

Ride-Sharing and Mobility-As-A-Service Trends

Autonomous vehicles will become more mainstream in the next several years, but not necessarily through traditional car ownership. It is likely that many first experiences with AVs will be with a rented or "shared" car.[34] The "sharing economy" and Mobility-As-A-Service ("MaaS") are trends that have grown over the past few years and are likely here to stay, if not increase in popularity.[35] KPMG's survey estimates that by 2025, more

[30] Autonomous vehicles fall on a spectrum of five levels, ranging from driver assistance to full automation where the steering wheel is optional. There are six levels, if you consider level 0, which is no automation. The National Highway Traffic Safety Administration (NHTSA) has created a five-level hierarchy. SAE International, Automated Driving: Levels of Driving Automation Are Defined in New SAE International Standard J3016, 2014, online: < https://www.smmt.co.uk/wp-content/uploads/sites/2/automated_driving.pdf>.

[31] Senate, Driving Change at 36.
[32] Rand, Guide for Policymakers at 75-76, and Lawson, The Connected Car.
[33] Lawson, The Connected Car at 29.
[34] Witnesses in the Senate Committee's study generally agreed that autonomous vehicles will likely be deployed in fleets (e.g., taxis, buses or delivery vehicles) and/or in environments where they can operate in a closed area. Senate, Driving Change at 27.
[35] The rental car industry purchases nearly 1/9 new vehicles sold in North America. Enterprise Holdings' Submission to Canadian Senate Standing Committee on Transport & Communication, at 2, online: <https://sencanada.ca/content/sen/committee/421/TRCM/Briefs/EnterpriseHoldings_TomiGerber_e.pdf>.

than half of all current car owners will not want to own a car,[36] but this trend will depend on factors like geography, ease of use, and availability.[37]

The decline in car ownership will disrupt the automotive industry, as well as our current conceptions of data privacy and data privacy laws. Because a single rental vehicle is supposed to have many drivers and occupants, fleet management companies have an advantage over manufacturers when it comes to the amount and types of data generated. Fleet management companies gather information faster than car manufacturers because the whole fleet gathers and pools the information. This "swarm intelligence" allows the self-driving technology to become safer, but also means more consumer and environmental data will be collected, stored, and generated, which, among other things, will complicate data ownership and control.

This data, whether personal or environmental, enables the development of MaaS and other platforms that aggregate transit and transportation data for mobility apps.[38] These trends in car ownership and transportation should not be overlooked when creating policy approaches to data privacy.[39] For example, we have already seen the issue of personal data not being wiped upon the vehicle's return to a rental agency.[40]

II. Data Ownership and Personal Data Management Will Be Among The Emerging Challenges To Data Privacy Laws

Policies for the data ownership and personal data management will be a challenge for regulators because there will be multiple organizations collecting, using and disclosing consumer data in jurisdictions all over the world. This is also an area where we will see a battle for data ownership between consumers and manufacturers, between

---

[36] KPMG, Survey at 25.
[37] Not surprisingly, younger consumers are more likely to agree that car ownership will decline. *Ibid* at 25.
[38] See, for example, Coord, a platform that aims to coordinate mobility platforms, navigation tools, and urban infrastructure. Coord is a spinoff of Sidewalk Labs, which is Alphabet's smart city venture. Stephen Smyth, "Announcing Coord: The integration platform for mobility providers, navigation tools, and urban infrastructure", Medium, (1 February 2018), online: < https://medium.com/sidewalk-talk/announcing-coord-the-integration-platform-for-mobility-providers-navigation-tools-and-urban-d0cd32d8526b>.
[39] In Japan, companies like Sony are getting into the ride-hailing business. Rather than ride-sharing, since Japan has banned using private cars for ride hailing services, Sony plans to use an AI-powered hailing platform to dispatch taxis. Jon Fingas, "Sony may launch an AI-powered taxi hailing system", Engadget (19 February 2018), online: < https://www.engadget.com/2018/02/19/sony-ai-powered-taxi-hailing>.
[40] Catherine Harrop, "Digital dirt: Why the data you leave in a rental car could threaten your privacy", CBC (26 January 2017), online: < http://www.cbc.ca/news/canada/new-brunswick/digital-data-left-in-cars-1.3948659>.

manufacturers and fleet operators and after-market providers,[41] and even between municipalities and organizations in circumstances where the vehicle and manufacturer benefits from being connected to government infrastructure.

There are four possible owners of in-vehicle data: car manufacturers; car owners; the individual whom the information is about and; the after-market applications that consumers or service businesses add to the car.[42] In a survey of customers, CAA asked customers who should have control and access to in-vehicle data and around 80 per cent of consumers believed they should have exclusive rights, while 3-8 per cent of responses were that automakers should have exclusive rights. Nearly 9 in 10 Canadians agree that the consumer should decide with whom the data should be shared.[43] KPMG's recent survey found that 84 per cent of consumers believed they should receive direct monetary benefit from their data, while 45 per cent of auto executives believed they need not offer anything in return for the data. KPMG's survey found that 49 per cent of consumers believe they are the sole owners of the data generated by the vehicle and they expect to receive benefits in exchange for their data.[44] While views on data ownership differ depending on regional and cultural differences,[45] these statistics show that many consumers expect some control and ownership over the data collected and generated.

The issues of ownership and access of the data is important because the entity that owns the data, as well as the messaging platform to the consumer, gains a controlled

[41] In a survey of stakeholders about who owned the data collected and generated by AVs, no one was sure who owns the data. See Rand, Guide for Policymakers at 94. The Canada Senate Committee also noted this tension in one of their recommendations. "Innovation, Science and Economic Development Canada monitor the impact of automated and connected vehicle technology on competition between the various sectors of the automotive and mobility industries, in order to ensure that sectors such as the aftermarket and car rental companies continue to have access to the data they need to offer their services." Senate, Driving Change at 14.

[42] In the analysis below "users" are defined as individuals who are in some way 'connected' to the vehicles either as a connected passenger with no contractual relationship with the vehicle's services[42], or is renting or 'sharing' it. Users may or may not be the owner of the vehicle. A "car owner" is meant to include both individuals and fleet management companies, like rental agencies.

[43] CAA, "Special Study on the Regulatory and Technical Issues Related to the Deployment of Connected and Automated Vehicles", (9 May 2017), p 15-16. Members Say is an ongoing market research study by CAA National. The survey addresses current issues relevant to CAA's various lines of business and public affairs initiatives. The final sample was 2,010 respondents.

[44] KPMG, Survey at 39-40.

[45] KPMG, Survey at 40.

messaging environment, which results in an advantage over competitors.[46] For example, consumers could be given recommendations for certain repair garages or restaurants without knowing why those particular ones were selected. Since MaaS and ride-sharing are likely to gain popularity, many vehicle manufacturers will make autonomous vehicles, as well as offer mobility services through them.[47] It is possible that just as a few social networking and consumer platforms control most of the data and communication, a few global companies could control most of the vehicles – and data - on the road.[48]

This illustrates that beyond data privacy concerns there are also competition issues. Access to data is crucial for small businesses, start-ups, and independent repair shops who want to provide after-market products and services to consumers.[49] This is why the vehicle rental industry and the Canadian Office of the Privacy Commissioner (OPC) both agree that a single sector, the manufacturer, should not alone control the in-vehicle data.[50] As a result of these concerns, the Senate of Canada recommended that while it is too early to know whether there will be anti-competitive behaviour, the situation should be monitored to ensure that the aftermarket sector and rental companies have access to the data to offer services.[51] Furthermore, since the data collected and generated by a connected car will be very useful in preventing and investigating car crashes, it is

[46] This ties in with the "right to repair" debates. In Canada, there is a voluntary "right to repair" agreement between manufacturers and the automotive aftermarket industry, the Canadian Automotive Service Information Standard (CASIS). CASIS is silent on telematics, but the Automotive Industries Association of Canada will work with vehicle manufacturers to avoid the closed-loop monopoly possible. The Association told the Senate of Canada that it is possible that regulation may be needed in the future. Senate, Driving Change at 59.
[47] See for example, Alison Griswold, "Waymo is readying a ride-hailing service that could directly compete with Uber", Quartz (16 February 2018), online: < https://qz.com/1208897/alphabets-waymo-googl-is-readying-a-ride-hailing-service-in-arizona-that-could-directly-compete-with-uber/>.
[48] Senate, Driving Change at 60.
[49] This is something the 2014 bill from California sought to address, see below, SB-327 Information privacy: connected devices. 1798.91.01., online: <https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB327>. California Small Business Association, noting that manufacturers having full control over the vehicle's data would help to level the playing field for small businesses Senate Transportation and Housing Committee on SB-994 Vehicles: vehicle information: privacy, April 22, 2014, at 1:47:00, online: < http://calchannel.granicus.com/MediaPlayer.php?view_id=&clip_id=2043&meta_id=16715>.
[50] Office of the Privacy Commissioner "Developing a Code of Practice for the Connected Car", (27 November 2017), p 7.
[51] Senate, Driving Change at 60.

possible that some types of data access will be mandatory, just as seat belts are mandatory now.[52]

Good Data Management Practices Are Good for Business

The multiplicity of organizations in the connected vehicle ecosystem will also present challenges for organizations to obtain informed, "non-fictional" consent from consumers.[53] For example, consumers buying or renting a car may not know that when they sign a purchase or rental contract that they are also providing consent to share their personal data.[54] Yet, consumers are becoming increasingly aware of how much personal information is being collected by organizations to offer services and for internal business or marketing purposes. Consumers are also aware of the never-ending stream of data leaks and breaches. Indeed, a survey by KPMG found that data privacy and security are a top priority for both purchasers of vehicles and for executives.[55]

A recent study on the negative effects of firms' data management practices suggests that when consumers are provided with transparent privacy policies and are given control over their data, they feel more empowered. [56] An example of empowering customers is allowing consumers to opt out of sharing their data with third parties or for certain purposes, like marketing. Empowered consumers are more willing to share information and are more forgiving of data privacy breaches. This is an important point because data

---

[52] Lauren Smith, "What's Driving the Connected Car? Data, It Turns Out", TEDxWilmingtonSalon, TEDx Video, 28 November 2017, online: < https://www.youtube.com/watch?time_continue=315&v=Fyz2GcdhQjQ>.

[53] Canada's federal private sector privacy law "assumes that individuals can give informed consent to the collection, use and third-party disclosure of their information." See Lawson, The Connected Car at 57.

[54] See for example, Peter Holley, "Big Brother on wheels: Why your car company may know more about you than your spouse.", (15 January 2018), The Washington Post, online: < https://www.washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse>.

[55] KPMG, Survey at 41.

[56] The research showed that the larger the breach and the more customers affected, the stock prices of rivals went up. This suggests that smaller breaches indicate that other organizations in the industry are vulnerable to breaches, while larger breaches gave consumers the impression that it was an isolated, unique occurrence. Kelly D. Martin, Abhishek Borah and Robert W. Palmatier, "Research: A Strong Privacy Policy Can Save Your Company Millions", Harvard Business Review, (15 February 2018), online: <https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions> [Martin, Research: A Strong Privacy Policy].

breaches also influence an organization's stock.[57] The study found that organizations that provide high levels of data transparency and control are insulated from the harms of consumers leaving and the spillover effects when a close competitor experiences a breach.[58] Interestingly, close competitors will be either harmed or helped by an organization's breach, depending on the size of the breach.[59] However, the research on the privacy policies of Fortune 100 companies found that 80 per cent of organizations did not offer transparency or control over data to consumers. The researchers found that "firms that failed to explain their data privacy practices had a 1.5 times larger drop in stock price than firms with high transparency."[60]

Consumers care about data privacy and the market is beginning to demand that organizations become more transparent about data collection and management practices.[61] Lengthy privacy policies are not the most transparent way to deal with the data privacy issues arising from autonomous vehicles. Organizations can profit while also respecting data privacy laws and empowering consumers. One way of empowering consumers, while allowing the organization to retain control of the data, is by providing consumers with a right to data portability.[62] This would allow consumers to request

---

[57] "Customers of firms that offer high transparency and control reported feeling less violated from big data practices, attested to being more trusting, provided more-accurate data to the firm, and were more likely to generate positive word of mouth." Martin, Research: A Strong Privacy Policy.
[58] Researchers poured through the privacy policies of all Fortune 100 companies and ranked their transparency and control given to consumers. "In 2011 Citigroup experienced a data breach of 146,000 customer records and suffered a $1.3 billion stock value loss. According to our analysis, if Citigroup had embraced practices of high transparency and high control, it would have suffered a loss of only about $16 million in stock value. That is, Citigroup might have saved about $820 million had it simply offered its customers high transparency and control." Martin, Research: A Strong Privacy Policy.
[59] "As the number of customers harmed by the breach increases, stock market effects for the firm's rivals go from negative to positive, as competitive effects become more dominant. This suggests that smaller breaches signal that others in the industry may also be vulnerable to hacking. However, large data breaches create the impression that the breached firm is in a unique amount of trouble." Martin, Research: A Strong Privacy Policy.
[60] *Ibid.*
[61] Some technology faces more hurdles than others in terms of consumer resistance and lack of adoption, such as Google Glass, or Peeple (the app that proposed to allow strangers to rate others without their consent). People inside and outside of the tech industry are commenting that the era of "permissionless innovation" must come to an end and that "technology is hijacking our minds and society". See, Center for Humane Technology, online: < http://humanetech.com/>.
[62] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art 20 [GDPR]. House of Commons, Bob Zimmer, Chair, "Towards Privacy By Design: Review Of The *Personal Information Protection And Electronic Documents Act",* Report of the Standing Committee on

their data from one service provider for the purposes of taking it to a competitor. Albeit more of a technical challenge, this is similar to allowing consumers to take their phone number to competing providers. Data portability may also facilitate competition between dominant players in the industry as well as encourage new entrants when trusted third parties, or secure data banks, hold and allow access to consumer data are used.[63] Just like copyright infringement, privacy is another form of intermediary liability which can result in financial losses. Respecting consumer privacy and protecting consumer data can also protect against financial losses and encourage VC investment.

III. Current regulatory landscape in Canada, the United States, and the European Union

This section provides a high-level overview of the current regulatory landscape in Canada, the U.S., and the EU. This section is not meant to be a comprehensive inventory of all the data protection laws, policies, directives, or bills pertaining to connected and automated vehicles. Rather, this section illustrates the main or most important approaches that these jurisdictions take to connected and autonomous vehicles to provide context for why a harmonized international framework is likely to occur and is largely beneficial.[64] While there are other laws and policies that may be relevant, the ones below were chosen to illustrate each jurisdiction's approach to privacy in general and as specifically related to connected and autonomous vehicles. Canada is often left out of discussions of international data privacy laws; thus, more detail is given to the legal and policy landscape in Canada regarding connected and autonomous vehicles.

Access to Information, Privacy and Ethics, February 2018, 42nd Parl, 1st Sess, at 83 [House of Commons, Towards Privacy By Design].

[63] This is because new entrants in the market would be allowed access to the (anonymized) data. Robert Seamans and Sam Himel, "Data Portability And Competition Between Technology Platforms", Forbes (6 March 2018), online: < https://www.forbes.com/sites/washingtonbytes/2018/03/06/data-portability-and-competition-between-technology-platforms/#191c65ab5bb5>.

[64] There is a difference between regulations, codes of practice, and standards. Regulations are mandatory obligations developed by policymakers and are enforceable. Standards are engineering criteria developed by the technology community and specify how the product should be designed. Codes of practice are voluntary principles and usually developed with input of all stakeholders. Standards are also voluntary, but both standards and codes of practice can become enforceable when they are incorporated into the law. See Rand, Guide for Policymakers, at xxii.

a) Canada

The Regulatory Landscape in Canada

In Canada, the starting point for commercial data privacy law is the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's private sector privacy legislation. It applies to organizations that collect, use and disclose personal information in the course of commercial activity.[65] This federal legislation applies to organizations in every province, except for provinces with substantially similar private sector legislation.[66] Provinces with data privacy laws must meet the minimum standards of privacy protection found in PIPEDA, but they can impose more stringent regulations. These differences between provincial laws and federal law will raise compliance costs and interoperability issues for vehicles that physically move between borders and for the data the vehicles send inter-provincially. PIPEDA defines "personal information" as information about an identifiable individual. This includes information on its own or in combination with other information that can be linked to an identified individual.[67] Not all data collected by a connected vehicle will be considered personal information and therefore will not be governed by PIPEDA. Some aspects of connected and autonomous vehicles will be regulated by sector. For example, insurance is provincially regulated in Canada, which means that the regulation of pay-as-you-go, or usage based insurance, is not federally regulated, except for what is caught by PIPEDA.[68]

The model of privacy protection in Canada is contract-based and aims to respect the personal autonomy of the individual who chooses to trade their personal information in return for services. However, privacy in Canada is also constitutionally protected vis-à-

[65]PIPEDA, s 4(1)(a). It also applies to personal information about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business. PIPEDA, s 4(1)(b).
[66] Alberta, BC, and Quebec have privacy legislation that has been deemed "substantially similar" to PIPEDA. However, while PIPEDA was given adequacy status under the EU's Data Directive, the provinces were not.
[67] "It does not matter who generated the information, or how, or who technically "owns" it." Privacy Commissioner of Canada, 2001-2002 Annual Report to Parliament, p 56.
[68] The British Columbia Privacy Commissioner recommended that Canada develop national data protection standards for usage-based insurance. Lawson, The Connected Car at 6.

vis the state in the *Charter of Rights and Freedoms*[69] and is also considered a quasi-constitutional right in the private sector.[70] It is interesting to note that PIPEDA came into being based on standards that were the result of broad consultations on the *Model Code for the Protection of Personal Information*.[71] These principles were implemented into law following consultations and international developments, especially those in the EU.[72]

PIPEDA also does not prohibit international transfers of data, but connected vehicle manufacturers and after-market providers who gain access to that data must abide by the principles found in PIPEDA, which provides the legal framework for organizations in Canada. [73] Some of these principles require a bit more explanation in the connected vehicle context. Organizations, especially ones that store or transfer personal information belonging to Canadians in or to foreign jurisdictions, should be especially

---

[69] See sections 7 and 8 of the *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11.

[70] For example, Canada's public sector privacy law, the *Privacy Act* was given quasi-constitutional status in *Lavigne v. Canada (Office of the Commissioner of Official Languages*), 2002 SCC 53. In a case regarding Alberta's privacy law, the Supreme Court of Canada also stated that "legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society": *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62. The Supreme Court of Canada stated that British Columbia's enjoy quasi-constitutional privacy protection in the recent decision of *Douez v. Facebook, Inc.* 2017 SCC 33. The Federal Court has confirmed in several cases that PIPEDA also has quasi-constitutional status. See *Eastmond v Canadian Pacific Railway*, 2004 FC 852 (CanLII), at para. 100; *Nammo v. TransUnion of Canada Inc.*, 2010 FC 1284, at para 75; and *Bertucci v. Royal Bank of Canada*, 2016 FC 332, at para 34. Early in the life of the *Canadian Charter of Rights and Freedoms*, the Supreme Court of Canada recognized that "the use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity": *R. v. Dyment*, [1988] 2 S.C.R. 417 at pp. 431-32.

[71] Miguel Bernal-Castillero, *Canada's Federal Privacy Laws*, Publication no. 2007-44-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 1 October 2013.

[72] For example, the EU passed a data protection directive in 1995 to ensure the protection of personal information while allowing the movement of data as necessary within the EU. The directive came into force in 1998. The directive required all member countries to adopt or modify existing national data protection legislation to comply with it. The directive extended its reach beyond the EU through Article 25 by prohibiting member countries (and businesses within them) from transferring personal information to any non-member country whose laws did not sufficiently guarantee the protection of that information. See European Parliament, Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995.

[73] PIPEDA incorporates ten privacy principles that were first codified by the OECD in its 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The ten principles are: Accountability, Identifying Purposes, Informed Consent, Limiting Collection, Limiting Use, Disclosure, and Retention, Accuracy, Safeguards, Openness, Individual Access, and Challenging Compliance.

mindful of four of PIPEDA's principles: accountability, openness, safeguards, and consent.[74]

Accountability means that the organization collecting the personal information of Canadians is ultimately responsible for the security and protection of that data, even when the data are stored in a foreign country or transferred to a service provider, parent company, or subsidiary in a foreign country.[75] Since organizations remain accountable for the data in another's care, organizations tend to use contractual clauses to require certain data practices to ensure that safeguarding standards are in place. Organizations must be open and transparent about the purposes for collection and use, whether the information will be disclosed and to whom, and the fact that once information is stored in another jurisdiction it is subject to the laws of that country.

Consent factors into the above principles in different ways. To comply with the principle of informed consent, organizations must understand the nuances of accountability and the law regarding transborder flows of data. A transfer of data is considered a use, not a disclosure. Thus, if the personal information is being used for the purpose it was originally collected, consent for the transfer is not required. If the transfer is for a different purpose to which the consumer had originally consented, the transfer is in contravention of the law.

As in other contexts, consent is not a black and white concept; there are grey areas and this is where organizations often struggle to comply.[76] For consent to be informed, the individual must be aware that providing consent is optional. Organizations cannot require consent for a purpose beyond what is necessary to supply the product or service.[77] This means that an individual cannot be denied use of the vehicle's normal

---

[74] Other principles are identifying purposes, limiting collection, limiting use, disclosure, and collection, accuracy, individual access, and challenging compliance. See PIPEDA, Schedule 1.
[75] PIPEDA, Schedule 1, s 4.1, cl 1, Accountability.
[76] The Office of the Privacy Commissioner, in its Annual Report, said these four elements should be included in privacy policies to obtain meaningful consent:
"what personal information is being collected; who it is being shared with, including an enumeration of third parties; for what purposes is information collected, used, or shared, including an explanation of purposes that are not integral to the service; and, what is the risk of harm to the individual, if any." OPC, *2016-17 Annual Report to Parliament,* September 2017, p. 20.
[77] PIPEDA, Schedule 1, "Principle 3 –Consent", cl. 4.3.

safety features because they opt-out of sharing personal information for infotainment or other non-essential services.[78] This practice is sometimes referred to as "tying", where a data processor links the terms in a contract to any use of personal data beyond which is necessary for the purpose of the contract.[79] Data controllers will also need to consider how to draft the legal and contractual restrictions to allow consumers to withdraw consent with reasonable notice, so that the user can still use the vehicle for its original purpose. Organizations must separate the necessary uses of personal data from the unnecessary and provide individuals the option to opt-out of unnecessary uses.

Consent can also be implied where it is reasonable to do so. Negative option, or opt-out consent for secondary purposes (such as marketing) is permitted, so long as the sensitivity of the information and reasonable expectations of the individual do not suggest otherwise.[80] Implicit consent for data when the risk of harm is low or non-existent may be the most appropriate consent model for connected vehicles. Users can also benefit from unanticipated uses of data, yet if explicit consent is required by data privacy legislation and it is difficult or impossible to obtain, then the consumer and the organization will lose out on the benefits. A Committee on privacy and ethics recently recommended that the federal government amend PIPEDA to explicitly require opt-in consent as the default for any use of personal information for secondary purposes.[81]

The Canadian Policy Approach

The Canadian Standing Senate Committee on Transport and Communications recently released a report based on its study on the regulatory and technical issues related to the deployment of automated (i.e. driverless) and connected vehicles.[82] The Committee concluded that all three levels of government must immediately plan for these

[78] PIPEDA, Schedule 1, Principle 3, cl. 4.3.3 states that "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes."
[79] See Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law", at 120 [Schwartz, Transatlantic Data Privacy Law].
[80] Lawson, The Connected Car at 77.
[81] House of Commons, Towards Privacy By Design, Recommendation 2, at 23.
[82] Senate, Driving Change.

technologies and provided 16 recommendations to the federal government.[83] The Committee recommended creating a national strategy[84] and it recognized that harmonized policies are important to attract developers, spur innovation, and protect Canadians.[85] The Senate Committee recommended that the federal government amend PIPEDA to give Canada's Privacy Commissioner power to proactively investigate and enforce industry compliance with privacy legislation.[86] The Committee also noted that there may be a need for privacy regulations specific to the connected vehicle and that a connected vehicle framework should be informed with the participation of relevant stakeholders.[87] However, even without binding regulations, a privacy framework for connected cars should be developed by all stakeholders. While the Committee suggested that sector-specific laws could be useful, it also recommended that Transport Canada work with the U.S. through the Regulatory Cooperation Council to ensure that vehicles operate seamlessly in both countries. [88] The federal Privacy Office is funding a Code of

[83] *Ibid* at 11. Autonomous vehicles and 'smart cities' share a similar policy and regulatory challenge in that many aspects will require cooperation between different levels of government. Canada's Constitution delineates certain powers to the federal government and provincial governments. Both levels of government have 'catch-all' powers which enable them to assert jurisdiction over different aspects of autonomous vehicles and smart cities. See, for example, the federal government's power in s. 91 (2) The Regulation of Trade and Commerce and the provincial power in s. 92 (10) Local Works and Undertakings, except those declared by Parliament as for the general Advantage of Canada or for the Advantage of Two or more of the Provinces and s. 92 (13) Property and Civil Rights in the Province. The federal government also has residual power for the Peace, Order, and good Government of Canada. *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11. Municipalities, as creatures of statute created by the province, will be directly involved in the benefits and challenges of autonomous vehicles and smart cities.

[84] The national strategy would involve several federal departments, including Innovation, Science and Economic Development Canada which aims to stimulate research and Transport Canada which focuses on vehicle safety. The Senate Committee recommended that Transport Canada work with two additional departments, the Communications Security Establishment and Public Safety Canada, to develop cybersecurity principles. Senate, Driving Change.

[85] *Ibid* at 11.

[86] *Ibid* at 11 and 57. The current approach is an ombudsman model, not an enforcement model. See House of Commons Report, at 54. The Privacy Commissioner noted that his office "can investigate only if it receives a complaint and argued that allowing his Office to act preventively – rather than reactively – would improve compliance with existing legislation." *Ibid*, at 56. The House of Commons Report also made the same recommendation to the federal government. See Recommendation 15 on the Privacy Commissioner's enforcement powers, "That the Personal Information Protection and Electronic Documents Act be amended to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance." House of Commons, Towards Privacy By Design.

[87] Senate, Driving Change at 14.

[88] *Ibid* at 13.

Practice for the Connected Car[89] and various committees and industry groups are establishing working groups and developing guidelines.[90]

b) The United States

The Regulatory Landscape in the U.S.

Personal information of US citizens is protected differently depending on the state and the sector. There is no federal data protection law that covers all commercial activity in all sectors and states. Instead, there are sector-specific laws for sectors like telecommunications, healthcare, and financial services, which tend to view privacy protection as consumer protection.[91] Consent is market-based: consumers are free to trade their personal data for benefits or convenience.[92] The U.S. does not have data protection authorities like the EU or a federal privacy commissioner like in Canada. Instead, privacy is enforced by consumer protection agencies, like the Federal Trade Commission[93], and by law enforcement agencies.[94] The FTC protects privacy in the U.S. generally under the umbrella of prohibiting unfair and deceptive methods, as well as

---

[89] Office of the Privacy Commissioner of Canada, "Privacy Commissioner announces funding for independent research projects on privacy issues", 16 May 2017, online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2017/an_170516_cp/.

[90] For example, AdChoices is a Canadian self-regulatory program for online behavioural advertising with dozens of stakeholders. See ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1600 (Adam Kardash, Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP, Interactive Advertising Bureau of Canada).

[91] "This Article finds that the EU system protects the individual by granting her fundamental rights pertaining to data protection. This language of rights creates a connection between data subjects and the EU institutions that safeguard these interests. By contrast, U.S. law protects the individual as a privacy consumer." Schwartz, Transatlantic Data Privacy Law at 121. This difference has also been noted in the Canadian context, where PIPEDA's consent model is ongoing, rather than a one-time transactional moment. Barrigar, Jennifer and Kerr, Ian R. and Burkell, Jacquelyn, "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information", (2006), Canadian Business Law Journal, Vol 44, online: <SSRN: https://ssrn.com/abstract=1303184>.

[92] See Schwartz, Transatlantic Data Privacy Law at 132.

[93] The FTC enforces the *Federal Trade Commission Act* and its with regards to data security and privacy arises from section 5 of the FTC Act which prohibits unfair and deceptive methods, acts or practices in or affecting commerce. U.S., 15 U.S.C. §§ 41-58, section 5.

[94] One of the FTC's divisions is the Division of Privacy and Identity Protection. FTC, Division of Privacy and Identity Protection, online: < https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity>.

through sector-specific laws, such as the *Children's Online Privacy Protection Rule*.[95] The FTC also has enforcement powers, which is different from Canada's Privacy Commissioner.[96]

The National Highway Traffic Safety Administration (NHTSA) and the U.S. Department of Transportation (USDOT) are the primary federal regulators of vehicle safety, and typically enacts Federal Motor Vehicle Safety Standards (FMVSSs) that specify performance standards for a wide range of safety components.[97]

AVs are also regulated state-by-state[98] and stakeholders from various organizations have expressed concern about conflicting state laws that it could restrict the deployment of AVs.[99] For example, California has relatively strong privacy legislation.[100] Its Constitution "gives each citizen an 'inalienable right' to pursue and obtain 'privacy'".[101] The *California Online Privacy Protection Act* (CalOPPA) applies to consumer websites and grants rights to consumers,[102] and may apply to some aspects of connected and autonomous vehicles, but there will be some regulatory gaps.[103] The California Civil Code uses the term "personally identifiable information" with the term defined narrowly and differently depending on the section's context and purpose. Other California laws,

---

[95] COPPA "imposes certain requirements on operators of websites or online services directed to children under 13 years of age". U.S., Children's Online Privacy Protection Rule ("COPPA"), 16 CFR Part 312.
[96] An FTC representative recommended to the House of Commons Committee that the Privacy Commissioner of Canada should have more enforcement powers. House of Commons, Towards Privacy By Design at 75.
[97] Rand, Guide for Policymakers at xxii.
[98] For a general overview of the laws in the US pertaining to AVs, see: Rand, Guide for Policymakers at 41; Lawson, The Connected Car at 85.
[99] Rand, Guide for Policymakers at 44.
[100] The House of Commons Committee commented that "Congressman Tony Cárdenas, member of the U.S. House of Representatives' Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce, and researchers from the Congressional Research Service mentioned that California is one of the most rigorous States in terms of privacy protection." House of Commons, Towards Privacy By Design at 70-71.
[101] United States (U.S.), State of California Department of Justice, Privacy Laws, online: <https://oag.ca.gov/privacy/privacy-laws>.
[102] Schwartz, Transatlantic Data Privacy Law at 136. Business And Professions Code – Bpc Division 8. Special Business Regulations [18400 - 22948.25], CHAPTER 22. Internet Privacy Requirements [22575 - 22579], online: < https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=>. See also, https://oag.ca.gov/privacy/privacy-laws.
[103] It applies to operators of commercial websites that collect personally identifiable information and requires website operators to conspicuously link to a Privacy Policy on their website. See generally, State of California Department of Justice, Privacy Laws, online: <https://oag.ca.gov/privacy/privacy-laws>.

federal laws, and laws of other states use different definitions with types of sensitive information protected, like credit card or social security numbers.[104]

In 2014, a bill was introduced in the California legislature to give consumers control over and access to the data collected by the vehicle[105], which the bill's sponsors saw as an extension of the control a consumer already has over the data collected by the car's event data recorder or other after-market devices added by the consumer.[106] This bill would have added another layer to California's privacy laws, but as it was intended to protect the privacy rights of "car owners",[107] we see a regulatory gap because it would fail to provide protection for those using ride-sharing services or MaaS. This bill did not become law. Interestingly, an automobile exception to the Fourth Amendment exists, where law enforcement officials can stop and search a vehicle based on probable cause without having to get a warrant from a judge.[108] These types of exceptions arguably no longer make sense now that vehicle store much more than physical items, like drugs or weapons. Other privacy laws, such as the *Electronic Communications Privacy Act*, may be applicable to some aspects of AV data privacy.[109]

The Policy Approach in the U.S.

---

[104] Determann, Lothar, Determann's Guide to Data Privacy Law: International Corporate Compliance, 3rd ed, Edward Elgar Publishing, Cheltenham, UK, at xxi-xxii [Determann, Determann's Guide].
[105] The bill would have required consumer consent for sharing or selling of personal information, and allow consumers to opt-out for the collection not necessary for the vehicle to operate safety and for manufacturers to tell the consumer what information will be collected and how it will be used.
[106] Referring to the car's black box. Alice Bisno, Senior Vice President for Public Affairs Automobile Club of Southern California, speaking to the Senate Transportation and Housing Committee on SB-994 Vehicles: vehicle information: privacy, April 22, 2014, at 1:44:40, online: < http://calchannel.granicus.com/MediaPlayer.php?view_id=&clip_id=2043&meta_id=16715>.
[107] Senator Bill Monning (D) Monterey, speaking to the Senate Transportation and Housing Committee on SB-994 Vehicles: vehicle information: privacy, April 22, 2014, at 1:36:40, online: < http://calchannel.granicus.com/MediaPlayer.php?view_id=&clip_id=2043&meta_id=16715>.
[108] For a discussion on the Fourth Amendment implications of autonomous and connected vehicles as they exist now or in the near future, see Lindsey Barrett, "Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception", Georgetown Law Journal Vol. 106:181, 181-208. But see, California Electronic Communications Privacy Act (CalECPA) - Penal Code section 1546, online: < https://oag.ca.gov/privacy/privacy-laws>. Which requires government entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.
[109] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22. The ECPA was intended to protect electronic communications stored on or transmitted by computers. The Drivers' Privacy Protection Act, and other federal statutes including the Federal Communications Act could also apply to certain aspects of autonomous vehicle data and communications.

California has an "IoT Bill" which aims to set reasonable security standards for connected devices offered for sale or sold to consumers in California.[110] Federally, the *Security and Privacy in Your Car (SPY Car) Act* of 2017 is a bill that proposes to regulate the privacy and security concerns stemming from CVs and AVs.[111] The FTC would have primary rulemaking authority under this Act for privacy standards, as it equates a violation of the privacy standards with "an unfair and deceptive act or practice" under the *Federal Trade Commission Act*.[112] The FTC could prosecute a violation and thus would operate as a federal enforcement agency.

The U.S. Department of Transportation announced a federal policy for autonomous vehicles which includes a 15-point safety assessment for vehicle manufacturers and a model policy for state governments.[113] There are also Automotive Privacy Principles[114] that went into effect for vehicles in model year 2017 and for subscription services beginning on January 2, 2016.[115] In addition to industry guidelines and regulation, educational guides for consumers play an important role. To this end, the Future of Privacy Forum and the National Automobile Dealers Association released a consumer guide to help consumers understand the types of personal data connected vehicles collect.[116]

---

[110] SB-327 Information privacy: connected devices. 1798.91.01., online: <https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB327>. "A manufacturer that sells or offers to sell a connected device to a consumer in California shall equip the device with reasonable security features appropriate to the nature of the device and the information it may collect, contain, or transmit, that protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." A "Connected device" is defined as "any device, sensor, or other physical object that is capable of connecting to the Internet, directly or indirectly, or to another connected device." SB-327 Information privacy: connected devices, online: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327>.

[111] For an in-depth discussion on the Bill, see Benjamin L. Bollinger, "The Security And Privacy In Your Car Act: Will It Actually Protect You?", North Carolina Journal Of Law & Technology, Volume 18, Issue On.: April 2017.

[112] Federal Trade Commission Act, online: <https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act>.

[113] U.S. DOT, "U.S. DOT Issues Federal Policy for Safe Testing and Deployment of Automated Vehicles," Press release, 20 September 2016.

[114] See AutomotivePrivacy.com

[115] National Automobile Dealers Association and the Future of Privacy Forum, "Personal Data In Your Car", (25 January 2017), at 6, online: <https://fpf.org/2017/01/25/fpf-and-nada-launch-guide-to-consumer-privacy-in-the-connected-car> [Personal Data in Your Car].

[116] *Ibid.*

c) The European Union

The Regulatory Landscape in the European Union

The EU takes a paternal approach to privacy and data protection that is expressed at the constitutional level and in regular law.[117] The EU aims to set the global privacy standard[118] with The Data Protection Directive,[119] which will be replaced by the General Data Protection Regulation (GDPR), on May 25, 2018.[120] The Directive did not prevent fragmentation of data protection across the EU or legal uncertainty as intended; these differences in data protection regulations are seen as obstacles to economic activities.[121]

The GDPR will regulate the data collected and generated in CVs and AVs in the EU and beyond, since it applies to the processing of personal data which have a link to the European Union's territory or market.[122] This means it applies to EU-based organizations, organizations that offer goods and services to EU residents, and organizations that monitor the behaviour of EU residents. Even organizations that collect or process personal information without a physical presence in the EU should assess whether they must comply.[123] Unlike U.S. data protection regulations, EU privacy laws apply to all sectors and industries. However, there are also sectoral laws which aim to bolster protection in certain areas, like telecommunications.[124]

---

[117] Schwartz, Transatlantic Data Privacy Law at 140.
[118] MEP Jan-Philippe Albrecht, "How the GDPR will change the world", 3 European Data Protection Law Review (2016). And see Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law", at 138. See also ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1620 (Jennifer Stoddart).
[119] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.
[120] GDPR.
[121] *Ibid*.
[122] *Ibid* Recitals 22-24, Arts 2-3.
[123] The costs of non-compliance are significant. There are two tiers of maximum fines depending on whether the controller or processor committed any previous violations and the nature of violation. Fines range from (a maximum of) 20 million euros to 4% of annual global turnover and the lower threshold fine is 10 million euros or 2% of annual global turnover, whichever is higher, as well as other administrative penalties and private legal claims. See Art. 83, Recitals 4 and 5 of the GDPR. Data Protection Authorities also have audit rights. Recital 148 authorizes a DPA to issue a reprimand in place of a fine in cases of a minor infringement where the fine would constitute a disproportionate burden on a natural person.
[124] Schwartz, Transatlantic Data Privacy Law at 128.

The GDPR applies to information concerning an identified or identifiable natural person.[125] It does not apply to anonymous information, which is information that does not relate to an identified or identifiable natural person, or that has been made anonymous so that the individual is no longer identifiable.[126] The GDPR also has a more robust concept of consent.[127] Consent must be clearly distinguishable, freely given, as easy to withdraw as it is to give, and auditable or verifiable. Consent must be unambiguous and not a passive activity, such as visiting a website with a pre-checked box to receive marketing emails. Importantly for connected vehicles, consent must be distinguishable. Consent cannot be included in a long privacy policy and consent for one use, like marketing, cannot be "bundled" with all types of consents. Providing an easy method for users to withdraw consent could be a challenge for connected vehicles, especially when considered with the fact that consent for marketing must not be a condition to receive the service. The GDPR recognizes a right to data portability, which is related to the principle of consent.[128] It will allow the consumer to request the transfer of their information from one provider to another. This right has implications for harmonizing standards between jurisdictions and organizations because organizations will need to ensure that their processes for collecting and storing personal information are sufficiently compatible with the processes used by competitors.[129]

The EU Policy Approach

The EU's Committee on Transport and Tourism recently released a draft report for a European strategy on cooperative intelligent transport systems. The report recommends that data generated from these systems be used for reasonable purposes and should not be retained or used for other purposes (presumably unless informed consent is obtained). These vehicles should also fully comply with the GDPR.[130]

---

[125] GDPR Art 4.
[126] *Ibid* Recital 26.
[127] *Ibid* Recital 32, Art 4.
[128] *Ibid* Art 20.
[129] House of Commons, Towards Privacy By Design at 36. The Committee recommended that a right to data portability be added to PIPEDA. However, Mr. Buttarelli, the European Data Protection Supervisor, in his appearance before the Committee, recommended that Canada not focus on "novelties in the GDPR, such as… data portability." ETHI, *Evidence*, 1st Session, 42nd Parliament, 13 June 2017, 1210 (Giovanni Buttarelli) at 1245 and 1250.
[130] European Parliament, Committee on Transport and Tourism, DRAFT REPORT on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI)), (16 November 2017), online: <

The EU Data Protection Directive[131] has already influenced data privacy laws in many jurisdictions[132] and data protection regulations around the world are being re-examined or drafted to fall in line with the EU's standard.[133] The EU intends to set a global standard[134] and pressure is mounting on both multinational companies and countries who seek to benefit from free-trade agreements with the EU.

IV. Factors and Trends for An International Data Privacy Framework

International Harmonization

Internationally harmonized data privacy laws are beneficial to industry in several ways. First, harmonized data privacy laws allow organizations to collect consistent data that can be aggregated. Second, harmonized laws reduce compliance costs and there is a reduced risk of contravention when laws are harmonized. Harmonization eliminates barriers to trade and makes business more efficient. For industry, adapting to updates and complying with differences in data privacy laws is an expensive and challenging task. Even differences in definitions, "personal information" for example, is another compliance cost for industry. Based on a recent survey, Global 500 companies will spend a combined $7.8 billion over the next year on GDPR compliance.[135] Data privacy compliance costs include hiring privacy professionals and implementing technical solutions. Compliance is further complicated when the data must be mapped and segregated depending on different uses. Third, there are indirect benefits to industry when consumers understand their data privacy rights, such as increased consumer trust

---

http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-610.712&format=PDF&language=EN&secondRef=01>.

[131] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31, Recital 9.

[132] See L Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014), at 208 (Kindle version).

[133] For example, Columbia, Argentina, South Korea, Israel, and Japan. Mark Scott and Laurens Cerulus, "Europe's new data protection rules export privacy standards worldwide", Politico, (31 January 2018), online: < https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation>. MEP Jan-Philippe Albrecht, "How the GDPR will change the world", 3 European Data Protection Law Review (2016), at 289.

[134] *Ibid*.

[135] According to a survey conducted by the International Association of Privacy Professionals (IAPP) and EY. Nicole Lindsey, "Global 500 Faces GDPR Compliance Costs of $7.8 Billion", CPO Magazine, (1 December 2017), online: < https://www.cpomagazine.com/2017/12/01/global-500-faces-gdpr-compliance-costs-of-7-8-billion/>.

and loyalty. Harmonized data privacy laws are generally easier for consumers because there are fewer conflicting rules of which to be aware when traveling or re-locating between jurisdictions.

Companies that operate in an integrated market, where standards for interoperability are important for function and for public safety, often find themselves subject to federally harmonized vehicle safety standards and emissions regulations.[136] Thus, industry has a role to play in setting technology-neutral standards or codes of practice.[137] Several national governments are also familiar with meeting the obligations of international data privacy laws and global harmonization initiatives regarding data privacy are not a product of modern society.[138] As noted, international considerations, coupled with stakeholder consultations, were part of the development process of Canada's PIPEDA. The House of Commons Committee on privacy and ethics also recommended that the Canadian government work with its EU counterparts to

---

[136] Rogers, Greg, "USDOT Unveils Ambitious Multimodal Automation Initiative, Automated Vehicles 3.0", Eno Transportation (9 March 2018), online: <https://www.enotrans.org/article/usdot-unveils-ambitious-multimodal-automation-initiative-automated-vehicles-3-0>.

[137] See, for example, Philippa Lawson, Barrister and Solicitor for BC FIPA, in Senate, Driving Change at 59.

[138] See, for example, 39th International Conference of Data Protection and Privacy Commissioners, "Resolution on Data Protection in Automated and Connected Vehicles", Hong Kong, 25-29 September 2017, p 2. The conference first convened in 1979 and has since been the global forum for data protection authorities with both open and closed sessions. Industry and academia participates in the open sessions. Since 2015, the U.S. and Canada have a connected vehicles work-plan to coordinate and collaborate on developing interoperable V2V and V2I technology. The G7 Ministers agreed to long-term cooperation coordinating research and the promotion of global standards "within an internationally harmonized regulatory framework" guaranteeing data protection and cyber security. Federal Ministry of Transport and Digital Infrastructure, "G7: Prosperity through modern infrastructure and Mobility 4.0", (21 September 2015), online: https://www.bmvi.de/SharedDocs/EN/PressRelease/2015/094-G7-wohlstand-durch-moderne-infrastruktur-und-mobilitaet.html. Transport Canada and the USDOT are the two departments involved. These initiatives are planned during the May 2016-December 2019 period. There are four initiatives: cybersecurity, spectrum analysis and allocation, standards and architecture, and information sharing initiatives and international events. Data privacy is included in the first initiative. See Transport Canada, "Canada-U.S Regulatory Cooperation Council (RCC) Connected Vehicles Work-Plan", (14 November 2016), online: <https://www.tc.gc.ca/eng/acts-regulations/tc-usdot-871.html>. However, going back even further, data protection authorities have been gathering at an annual conference since 1979. The goal of this conference is to provide leadership at an international level in data protection and privacy International Conference of Data Protection and Privacy Commissioners, "About the Conference", online: <https://www.privacyconference2017.org/eng/about_the_conference.html>. Similarly, The World Forum for Harmonization of Vehicle Regulations (WP 29) has been in existence for more than 50 years and as the name suggests, it works to harmonize global regulations on vehicles. United Nations Economic Commission for Europe (UNECE), World Forum for Harmonization of Vehicle Regulations (WP 29), "Introduction", online: <https://www.unece.org/trans/main/wp29/meeting_docs_wp29.html>.

determine how Canada could achieve adequacy status with the GDPR.[139] Furthermore, since the transborder flow of data has become a business reality and the EU law allows personal data to flow outside the EU only if there is an adequate level of protection in the destination country or if specific exceptions apply,[140] some countries already harmonize national laws with the EU to ease compliance concerns for organizations that operate internationally. For example, Canada's federal private section legislation, PIPEDA, met the EU's adequacy standard for its soon-to-be-superseded Data Protection Direction and thus was already "harmonized" with the EU law.[141] There is some uncertainty about whether PIPEDA will meet the adequacy requirement after the GDPR comes into force on May 25, 2018. Canada has not yet moved to amend its law; however, considering its past movement to harmonize, it is very likely that Canada would amend its law to meet the EU's new standards if necessary. The House of Commons Committee on privacy and ethics also provided several recommendations addressing this issue.[142]

Practically, it makes sense for regulations to be harmonized, because a patchwork of incompatible requirements or standards would make it functionally impossible to operate a vehicle in multiple jurisdictions.[143] To this point, and to encourage the deployment to AVs, the U.S. Department of Transportation ("USDOT") AV policy included the principle that the USDOT will work with states and other entities to avoid patchwork regulations that could impede AVs crossing state lines.[144] However, it is also true that different cultural approaches to the concept of privacy and data protection are a major hurdle in harmonizing laws and creating standards. The differences between the U.S. and the EU's legal approaches to data privacy is one example, which has been termed the "transatlantic data war".[145] These differences may be aggravated by what has

[139] House of Commons, Towards Privacy By Design, Recommendation 17, at 69.
[140] The transfer of personal data to third countries and international organisations by EU institutions and bodies, Position Paper, Brussels (14 July 2014).
[141] The 1995 Data Protection Directive incorporates the "ten privacy principles" originally set out in the OECD's 1980 Privacy Principles. Canada's federal private sector privacy law also incorporates these principles.
[142] House of Commons, Towards Privacy By Design, Recommendations 17-19.
[143] This is something federal governments already recognize. See Rogers, Eno Transportation.

[144] *Ibid.*
[145] Henry Farrell & Abraham Newman, The Transatlantic Data War, FOREIGN AFFAIRS (Feb. 2016), online: https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war

been termed as the "Trump Effect", which may destabilize relations between the U.S. and the EU.[146]

Other Ways to Regulate AVs And Data Privacy: Sector-Specific Laws And Codes Of Practice

As noted, some jurisdictions, like the U.S., take a mostly sectoral approach to data privacy laws. Sector-specific regulations also arise when the industry or technology present unique challenges and a law of general application would not be appropriate. For instance, the GDPR recognizes that Member States may have sector-specific laws in areas that need special attention. This can also mean specifying rules for special categories of personal data.[147]

However, there are often regulatory gaps in sector-specific laws, for example when it is difficult to define where the connected vehicle sector begins and ends or when the laws are too specific and not technologically neutral. Sectors like healthcare or insurance are easier to regulate with sector-specific regulations or codes of practice because these sectors are easier to distinguish from other sectors.[148] Sector or technology-specific laws can also become outdated when technology evolves and this can create compliance challenges for industry. Harmonized data privacy regulations of general application do not have these limitations. The Privacy Commissioner of Canada opines that sector-specific legislation is "likely to place limitations on valuable business uses of data that may not in fact violate privacy."[149] Many of the goals of sector-specific regulation can be met through codes of practice or industry standards.

[https://perma.cc/6CGM-SMPH. And see Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law", at 117.

[146] Schwartz, Transatlantic Data Privacy Law at 120, 138, and 171-173. For example, Congress recently rolled back strong privacy protections from the Federal Communications Commission (FCC). The rules sought to extend the FCC's privacy protection to ISPs, termed "broadband Internet access services." FCC, Notice of Proposed Rulemaking 2500, 2506 FCC 16-39 (Apr. 1, 2016) and *ibid* at 138.

[147] GDPR, Recital 10.

[148] OPC, Code of Practice at 5.

[149] *Ibid* at 7. But see, Alan McQuinn, "Privacy advocates are wrong on connected cars", The Hill (3 February 2018), online: < http://thehill.com/opinion/technology/372186-privacy-advocates-are-wrong-on-connected-cars>.

The Canadian Privacy Commissioner suggested that codes of practice or regulations could regulate data categories in the provision of connected vehicle services. The data could be split into six categories, such as infotainment data[150], driver behaviour, and biometrics.[151] "By developing principles around categories of data rather than organizations or industry sectors, consumers can better understand the type of data involved."[152] This could also provide predictability for organizations in terms of understanding their obligations regarding consent as well as the appropriate limits on data processing.[153]

Standards are often developed by industry, interest groups, and standard-setting bodies to specify how a product should be designed or how it should perform. Guidelines can also be developed by policy-makers working with industry to develop codes of practice.[154] Standards, principles, and guidelines are examples of self-regulation that can be useful for industry and consumers.[155] Industry can also get creative and create apps

[150] Such as music selection or mobile applications.
[151] The six categories of data generated by a connected vehicle are: "1. Infotainment data is generated by the infotainment system (such as music selection or mobile applications) 2. Personal communications data is generated by messages sent or received via the vehicle infotainment system (this is often done through a synched smartphone. 3. Location data concerns data about a vehicle's location at any given time 4. Driver behaviour refers to when and how a driver operates the vehicle 5. Biometrics and health concerns data gathered by health monitoring devices in or linked to the vehicle and 6. Vehicle diagnostics is data generated by a vehicle's internal systems on the performance of vehicle components." OPC, Code of Practice at 8. See also PwC, "In the Fast Lane: The Bright Future of Connected Cars", 2014, at 8 for six categories of distinct products categories: mobility management, vehicle management, entertainment, safety, driver assistance, and well-being.
[152] OPC, Code of Practice at 8.
[153] *Ibid* 8.
[154] Ann Corvoukian, the former Privacy Commissioner of Ontario, recently launched a global council focused on privacy by design. See International Council on Global Privacy and Security by Design, online: < https://gpsbydesign.org/>.
[155] See for example, The Time Well Spent movement, which has proposed a "Hippocratic Oath for technology": *first, do no harm*. Center for Humane Technology, online: < http://humanetech.com/>. See also, Jessica Galang, "FIGURE1'S JOSHUA LANDY SAYS WE NEED A HIPPOCRATIC OATH FOR TECH", Betakit (5 March 2018), online: < https://betakit.com/figure1s-joshua-landy-says-we-need-a-hippocratic-oath-for-tech/>. And the Manila Principles on Intermediary Liability. Manila Principles on Intermediary Liability, online: < https://www.manilaprinciples.org/principles>. See generally, Giancarlo Frosio, "Welcome To The Manila Intermediary Liability Principles!", The Center for Internet and Society Stanford Law School, Blog, online: < https://cyberlaw.stanford.edu/blog/2015/03/welcome-manila-intermediary-liability-principles>.

for users to query a chatbot about the privacy settings of the vehicle and this may be a good move for organizations aiming to educate the user and obtain valid consent.[156]

V. Conclusion

It is too soon to develop broad-sweeping regulations, but the AV industry requires direction. While governments should not make regulations without first identifying the harms and considering the effects of regulations, including how it could stifle experimentation and innovation, this does not mean we should use a wait and see approach. Experts in both Canada and the U.S. have separately concluded that guidance to inform automaker's actions and protect consumers' privacy should be improved.[157]

Standards and guidelines should be approached like navigation apps that provide several routes, each optimized to address a particular challenge, be it privacy or safety. It may be too early to know whether voluntary codes of practices will be enough, or if specific data privacy regulations will be required.[158] However, binding rules with enforcement mechanisms and penalties are likely required in some areas, like data leaks and breaches.[159] Nonetheless, standards and guidelines from industry groups and government are a useful starting point to provide direction for industry, and to set consumer expectations. Privacy and data protection specialists will also have a role in

---

[156] See "Daimler unveils new 'Ask Mercedes' customer service chatbot", Reuters, (7 November 2017), online: < https://www.reuters.com/article/us-internet-europe-daimler/daimler-unveils-new-ask-mercedes-customer-service-chatbot-idUSKBN1D72AU>; and Andy Greenberg, "AN AI THAT READS PRIVACY POLICIES SO THAT YOU DON'T HAVE TO", WIRED (2 February 2018), online: <https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/>.

[157] Submissions from the Office of the Privacy Commissioner to the Standing Senate Committee on Transport and Communications, referencing the US Government Accountability Office's (GAO) report on vehicle data privacy and a study by the British Columbia Freedom of Information and Privacy Association, funded under the OPC's Contributions Program. See "Submission to the Standing Committee on Transport and Communications regarding their study on the regulatory and technical issues related to the deployment of connected and automated vehicles", (28 March 2017), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_sub_171122/>.

[158]The Senate Committee believes it is too early to determine this. However, the government should bring together all relevant stakeholders to develop a framework. Senate, Driving Change at 59-60.

[159] Also see Ryan Calo cautioning that organizations dominating the AI industry will prefer standards over regulations because of the lack of bite in the former: "Artificial Intelligence Policy: A Primer And Roadmap", Calo, Ryan, Artificial Intelligence Policy: A Primer and Roadmap (August 8, 2017), at 7, online: <SSRN: https://ssrn.com/abstract=3015350 or http://dx.doi.org/10.2139/ssrn.3015350>.

advising and compliance, to implement privacy by design, and for clean up after the inevitable breach.[160]

A harmonized legal framework provides a level playing field for organizations around the world and is a positive for both industry and consumers. A regulatory framework should, when necessary, have some bite, yet be adaptable and flexible to allow innovation and experimentation. A framework should include a mix of binding regulations as well as industry standards and code of practice. This framework should be developed by addressing the short-term challenges of connected vehicles while allowing experimentation of advanced technology like AVs. We can promote innovation and encourage adoption of AVs, while planning for the data privacy challenges of the long term when cities become "smart" and autonomous vehicles are mainstream.

[160] See this webinar of a recent ransomware attack on the University of Calgary. The webinar details the attack, how the University responded, and tips for other organizations. Having a breach coach on retainer is one recommendation. The Conference Board of Canada, "Beware Ransomware: Learning from the University of Calgary Ransomware Case", (20 June 2017), online: < https://www.conferenceboard.ca/e-library/abstract.aspx?did=8851>.