A Code of Practice for Connected Vehicles

One Page Synopsis

The aim of this project is to develop a privacy code of practice for the connected car. The purpose of the code is to draw attention to inappropriate data handling practices that may otherwise go unnoticed and assist individuals in understanding the data they are entitled to control.

The expectation is that a code of practice would provide an added measure of predictability and consistency for companies in terms of understanding their obligations around meaningful consent and appropriate limits on data processing as well as provide greater clarity for individuals regarding how their data is being processed.

This research is motivated by the fact that privacy protection addresses isolated transactions between individuals and organizations. This approach to privacy protection, which relies on individual consent regarding the collection, use, and disclosure of data, fails to take into account the increasingly interdependent nature of privacy and the complex nature of information networks. As a result, the over-reliance on consent as the mechanism by which consumers control access to their personal information is becoming increasingly untenable.

While prescriptive rules in the connected vehicle context would be easy to justify if the uses of data had little or no benefit or were otherwise harmful, there are many socially desirable uses of connected car vehicle data such as location-based services or vehicular diagnostics.

However, by placing boundaries on the sharing of location data by third parties, for example, as well as softer default rules on the use of non-personally identifiable information, it would be easier for individuals to appreciate how their privacy is being protected. It would also enable individuals to demand services to be provided in more minimally intrusive ways.

Questions for discussion

1. What are your privacy concerns concerning connected vehicles?
2. Would consumers ultimately benefit from implementing a code of practice?
3. What, in your view, would be the likely economic consequences of implementing a code of practice in this sector?

The following responses were provided from members of the Privacy Access Council of Canada

1. What are your privacy concerns concerning connected vehicles?

It is important to understand that connected and self-driving are not necessarily the same thing: self driving cars need not be fully "connected". Most cars on the road right now are "connected" in some way, but there is no necessary relationship between connectivity and self driving technology.

Self-driving cars can (should) be built to communicate with other vehicles (V2V) or other infrastructure (V2I), and can (should) be designed to operate independently of any other technologies.

Privacy considerations are different between individually owned vs. fleet managed vehicles. In a fleet model, when vehicles are shared, the universe of privacy-sensitive data becomes more clear. And as shared self driving vehicles become a reality, this narrows further -- e.g. telematics data from an OBD-II port will be less indicative of driver behavioral characteristics.

Just how interconnected will connected vehicles be with the rest of an individual's real life. Assuming there are significant analytics, who owns that data and how is it protected? How will it be anonymized since vehicles are registered to an individual, making the data generated by a vehicle easily trackable to the registered owner?

Will all data generated by a vehicle be attributed to the registered owner or will/can data generated by a vehicle — when it is not the registered owner driving it — be distinguished somehow?

Who is the driver - the automation behind the wheel or the licensee who pays for the vehicle/trip? Who gets direct and indirect access to that information or parts of it (which parts?, and who decides?)?

Who is responsible for the data collected, automation or human functions?

Who is responsible for liability? How do you penalize an automated system?

I am concerned that a faceless person (or perhaps an insurance company or even the government) will have access to and use information regarding individuals' whereabouts, driving behaviors, and perhaps even their passengers for nefarious purposes or simply for purposes for which they do not require the information (and perhaps sell the information). It is also conceivable that private conversations or what radio programs/podcasts, etc. individuals listen to in the vehicle could also be

captured (since we know that this is happening already through our smart phones and computers).

There is a danger that, over time, information may be seen as "required" (e.g. by insurance companies) simply because it is now available when it was previously not "required". Even if the information is truly required for a legitimate purpose by the party collecting it, there is also a risk of hackers obtaining access.

I am concerned about the significant safety risks if the vehicle is remotely controlled.

The amount of data related to me (the driver or the primary user), passengers, and also the data tracked of the trips. Unauthorized users could gain insights into frequency, locations of school/work and patterns of absences away from home, creating the potential for personal harm where none existed before but for the logging of people's travels.

Will the data collected be openly described in a Terms & Conditions with users? For example, users can control the data they share on Facebook via privacy settings but users have zero control over how much data Facebook collects.

I am concerned that Terms and Conditions on automakers' websites are general, at best, and offer no real idea of just who does/will have access to data generated by my vehicle. Vague labels such as "partners" and "affiliates" aren't helpful, and could mean anything from advertisers to governments.

What data will be allowed to be collected, and for what purpose? As it is, the "purpose" for data collection is stated in remarkably general terms: for 'business purposes or as required by law'. Business purposes could be to enable the company collecting the data to sell it, give it to anyone they wish, or hand it to the government without consent — because it's collected for a 'stated purpose'. Drivers and passengers need to know just where their information is going to be able to have any control over it. How will a voluntary code of conduct make that happen?

Who owns what data, and what jurisdiction does it resides in? Unless the data is required, by law, to be retained within Canada, Canadians will be unable to exercise their right to gain access to their personal information collected by the vehicle.

How will a code of conduct for automakers help people and their data be safe from imperfect security used by automakers and component makers? How will a code help prevent malicious events and cyber-hijacking of vehicles?

How will self-driving cars resolve ethical issues as they arise? E.g., a pedestrian jay-walking or a car runs a yellow/red light but a pedestrian is crossing. Will the self-driving car hit the car or the human? Can AI solve this?

If AI is allowed to continue to be shielded from examination by claims of commercial confidentiality, there will be no way to interrogate a vehicle's systems to ascertain liability after collisions, breakdowns, or in relation to data.

Data and metadata opt-outs should be available for users of connected vehicles, at a granular level, regardless of who owns the vehicle. If I'm in a vehicle as driver or passenger, I should have a way to control the collection, use and dissemination of all data gathered from/about me, the devices (smart phones, tablets etc.) I might have with me, and the vehicle itself.

The data retention policies of the manufacturer/operator need to be explicitly communicated (not just posted somewhere on a website) and should (by law) not be allowed to be vaguely-worded licenses for perpetual retention. Existing assurances that "We will only keep the information as long as necessary for legal or business purposes" allows an organization to retain information in perpetuity. And since consent to terms and conditions is now an all-or-nothing deal (you buy the car, you agree to all the vague and hidden terms and policies that imply your information will be collected by the auto company and shared with whomever it wishes) and since corporate policies are internal documents, the private companies have no obligation to reveal the precise wording of internal communications or policies — leaving consumers in the dark.

I am concerned about the sharing of data with auto insurance and life insurance providers and the Ministry of Transportation.

Rather than concerns, per se, I am offering what I would like to see in a code of practice:

- Explicit recognition that vehicle information may constitute personal information about the driver and/or registered owner.
- Recognition of the application of PIPEDA to vehicle data, inasmuch as the vehicle data arise from the purchase of the vehicle. If this proves difficult (it could be argued that it is a bit of a stretch), I would prefer to see the code of practice eventually enshrined in law, perhaps as a regulation to PIPEDA.
- No release of vehicle information by the manufacturer to any third party without explicit consent of the owner or a court order, except in cases of imminent risk to health or safety.
- Communications with, and services to, the owner of record do not require consent. Nor do software updates to vehicle systems, provided such updates

are made to all vehicles for a given model, year and trim level (i.e., no vehicle-specific software updates, such as at the request of law enforcement).
- Consent for access to vehicle data cannot be a condition of insurance or registration. The blanket consent of the owner to third-party disclosures by the manufacturer cannot be a condition of the sale of the vehicle.
- All telemetric data to be encrypted in transit.
- Vehicle data recorders should use encrypted storage as well. (I would have to think about how best to implement that in a way that the data are available to service technicians if necessary. Encryption keys would have to be vehicle-specific for encryption to be of much use, but that could complicate servicing.) Without effective encryption, law enforcement (and perhaps others) could circumvent the code of practice by impounding the vehicle and interrogating the recorder(s). I would prefer that they be required to have a court order to obtain the encryption key from the manufacturer.
- Ideally, I would like to see telemetric data stored in the country in which the vehicle is sold, but manufacturers would resist that strongly.

2. Would consumers ultimately benefit from implementing a code of practice?

Yes - however only if the code is enforced. Penalties would have to be imposed for infractions. Enforcement and penalties would have to be consistent across the country.

Absolutely, the industry needs appropriate guidelines and how to protect consumers. Inevitably, though, what consumers consider 'appropriate' might be entirely different from what automakers and governments consider 'appropriate'.

A code of practice usually has ethics and contingencies, how can an automated system apply imperfections in the standard?

Most definitely. I encourage and embrace innovation but the Government of Canada must regulate appropriately to protect citizens. There needs to be clear transparency around the type of data and metadata collected, sharing, corporate partnerships, data storage and retention policies.

Recognition of both individual and manufacturer rights and obligations associated with vehicle data, especially telemetrics and vehicle operation records. Limitations on third-party access to vehicle data without clear authority. Realistically, I don't think you can limit manufacturer access to the data.

Maybe, if it can conduct prevent our information from being siphoned off to become part of our data shadows or traded amongst data brokers.

Yes, but only if it helps us know what people/entities our information is given to or shared with.

Yes, but only if complying with a code is mandatory. Automakers already have a voluntary code of practice for motor vehicle advertising, which stresses that adherence is entirely voluntary. Without mandatory requirements to adhere to a strict code of conduct that protects consumers' information (not the company's bottom line) the auto industry, which is resistant to being limited and is a heavily funded lobby group, will have no incentive to change to improve privacy or provide people with any greater data control than they now have (which is none).

3. What, in your view, would be the likely economic consequences of implementing a code of practice in this sector? Please consider short term, long term, positive and negative impacts.

Any additional rules which are imposed carry an economic cost; however, failure to impose rules carries an even greater societal cost. I would suggest that those that benefit from the technology (i.e. manufacturers and those with direct and indirect access to the information obtained from the technology) should bear the economic costs (although I am not naïve enough to think that those costs will not ultimately be passed on to consumers who do not necessarily want the technology but are forced to buy it when it is included in their vehicle).

Thinking about privacy at beginning stages (i.e. privacy by design) should just be the cost of doing business.

Short term - WIFI does not always work in the car, towers are down in remote areas, example there is a dead spot on the highway from Calgary to Red Deer at Gasoline Alley this could potentially cause an accident.

Long term - Direct driver input to control steering, acceleration and braking means that the driver still must be aware and fully cognizant. What happens when they fall asleep, use computer or cell phone?

Positive - Turnkey for automakers increasing profits, GDP and new jobs for technical graduates.

Negative - Sharing internet access to other devices is worrisome, travel logs - entice suspicious activity, following a woman at night, allows burglars to know when homeowner is away.

Short term - Implementing a code of practice could influence user adoption, positively or negatively.

Long term - Compliance and enforcement of the code of practice to ensure it meaningfully protects the customers/users and the suppliers/auto manufacturers.

Positive - To demonstrably improve data, privacy and security in the intelligent vehicle industry.

Negative - The length of time to develop a common code of practice agreeable to all stakeholders: government, safety councils, auto manufacturer(s), etc.

Negative - Could raise vehicle prices.

Negative - Manufacturers might have (or claim to have) new costs associated with supporting law enforcement and insurers if full encryption is implemented, and those would be passed on to consumers.

It's not economic, but I expect there would be political resistance to a code of practice from manufacturers and, perhaps, foreign and domestic governments (some of which would not want limitations on law enforcement access).