Comparing Privacy Codes of Practice in the Connected Vehicle Industry

By: Mathew Coe

Project Overview

Addressing privacy concerns are seen as central to the widespread adoption of connected vehicles. However, there is a fundamental disconnect between current privacy laws, which rely on consumers being able to make informed decisions regarding the sharing of personal data and the use of that data in commercial contexts. This is particularly true in the case of connected vehicles where there is a vast amount of data being shared between a wide range of commercial and government entities as well as consumers. In order to address this issue the use of privacy codes of practice have been proposed. This project compares different privacy codes of practice that have been developed for the connected car industry. The aim of this project is to assess the relative strengths and weaknesses of these codes for the purpose of consumer privacy protection.

Introduction

Modern vehicles are much more complex than they were fifty, twenty or even ten years ago. Today's vehicles are essentially smartphones on wheels. They are capable of communicating with their internal systems, other vehicles and local infrastructure. This communication can provide many amazing features such as safety, mobility and onboard infotainment. But to provide all these features a great deal of information will be gathered, some of that information will be "personally identifiable". The distinction between data and personal identifiable information is important, because one can help advance the world around us, while the other in the wrong hand can affect our personal privacy and animosity. The industry must look at how personally identifiable information is handled and how consumers can participate through consent. One of the ways the industry can do that is through a "code of practice". A code of practice is a written set of rules on how a profession should act, that is accepted by one or many

Code of Conduct Disadvantages

1) If not continually enforcement can simply be ignored

2) Opens companies up to litigation or bad publicity

3) Can be costly to create and to publicize and may not even be adopted in the industry after these costs are incurred

Code of Conduct Advantages

1) Transparency for consumers, allowing them to make informed decisions

2) Reduce unwanted future regulations imposed by the government

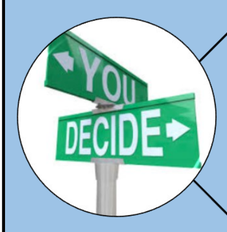
3) Governments save time and money not having to impose legislation demanded by public scrutiny.

Code of Conduct Analysis

ACEA

TRANSPARENCY

1. Inform customers about the personal data that we process.
2. The purpose we use them for.
3. The third party we may share them with
4. Information must be available in a clear, meaningful and be easily accessbile
5. Inform clients of any changes to policy
6. Provide contact points where customer can obtain information about the personal data we process



CHOICE

1. Aim so that vehciles/services give the options to customers whether or not to share personal data
2. Third party data usage may only be used with consumer consent
3. De-activation of geolocation features except for emergency situations

DATA PROTECTION / DATA SECURITY

1. Data protection requirements must be taken into account when creting new products/services
2. Where important data may be obtained must conduct a data protection impact assessment
3. Implement appropriate technical, security and organisational measures to protect the personal data of customers
4. All outsorced data process will be imposed by contractual safeguards

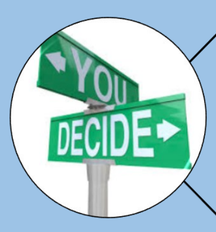
DATA PROCESSING

1. Only necessary data will be used for the purpose intended
2. Anonymisation, pseudonymisation and de-indentification are important mechanisms for protecting personal data
3. All personal data will be considered personal even when combined with other data
4. Any personal data that no longer serves it orginal purpose will be deleted, blocked or rendered anonymous

AUYO ISAC

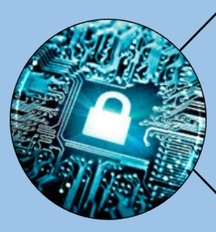
TRANSPARENCY

1. Provide notice through owners' manuals, paper/eletronic forms and in-vehicle displays
2. Provide notice prior to initial collection of covered information
3. Notices will contain, type of information collected, the purpose, the entities the information is shared with, the deletion of information, consumer choices
4. Geolocation, biometric and driver behavior information member commit to provind clear, meaninful and prominent notices about collection of such information



CHOICE

1. Information pertaining to safety may collected without choice
2. Particpating members must obtain consent for sharing and using geolocation, biometric and driver behaviour information
3. Consent may be obtained at the time of vehicle purchase/lease, or when registering for a product



DATA PROTECTION/ DATA SECURITY

1. Implement standard industry practices

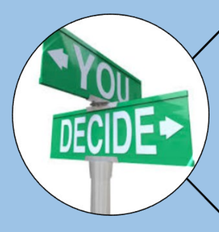
DATA PROCESSING

1. Only necessary covered information will be used for the purpose intended
2. Covered information will not be retained longer then necessary for business purposes

SMMT

TRANSPARENCY

1. Inform consumers on the personal data, that is processed
2. The purposes for which the data is used
3. The third party, with whom the data may be shared
4. The identity of the company or group that governs the data processing
5. Customers will be informed of any changes to manufacturers' privacy policies



CHOICE

1. Manufacturers commit to giving customers the choice, where possible, of whether to share personal data; obtaining customer consent for sharing the data with third parties
2. Allowing customers to de-activate the geolocation functionality of the vehicle

DATA PROTECTION / DATA SECURITY

1. Manufacturers commit to maintaining high levels of data protection when designing and developing new products, services and processes, including, if necessary, carrying out data protection impact assessments
2. Compliance with the EU General Data Protection Regulation principle of "privacy by design"

DATA PROCESSING

1. Manufacturers commit to processing only personal data that are relevant and retaining the data for only as long as it is necessary to fulfil the purposes for which it is collected
2. Manufacturers also anonymise and de-identify personal data where appropriate, as these are considered important mechanisms for protecting personal data

Recommendation

Each code of practice has some areas of strengths and some issues that need to be addressed. For Transparency the AUTO ISAC was the only one to directly address the main issues concerning data privacy geolocation, biometrics and driver behavior information. For choice ACEA gave the most power to consumer with a De-activation feature on all geolocation features. Under choice the AUTO ISAC was weak as choice is given up at the point of consent (signed contract) this can be problematic for consumers. For Data Protection/ Data security I don't think any code hit the mark. Lastly, Data Processing all were very good, but ACEA started to look at what happens with data when it is combined with other data. In conclusion the ACEA has the strongest points, but there the other two should also be taken into consideration.

Conclusion

Weighing the pros and cons, I believe sectoral codes of practice could indeed help consumers, the industry and different levels of government. Companies will need to do their due diligence for creating a unified code of conduct because if not implemented correctly and enforced there can be drawbacks. To make sure Canada implements a well-defined code of practice it is wise to look at other codes of practice abroad and use what they did well and what they did not.