

DRIVER EDUCATION, TRAINING AND ROAD SAFETY

Name: Dr Elizabeth Coombs
Organisation: Office of the Privacy Commissioner NSW
Date Received: 8/12/2016



office of the
privacy
commissioner
new south wales



Mr Greg Aplin MP
Committee's Chair
Joint Standing Committee on Road Safety
Parliament House
Macquarie Street
SYDNEY NSW 2000

Our reference: **IPC16/A000381**

- 8 DEC 2016

*via- email to: David Hale, Main Contact
staysafe@parliament.nsw.edu.au*

Dear Mr Aplin

Submission to inquiry into driver education, training, and road safety

I write to provide you with my submission to the Legislative Council's inquiry into driver education, training, and road safety.

The aim of this submission is to illustrate current and emerging vehicle technologies and their privacy implications as well as the need for organisations and entities to implement a "Privacy by Design" approach from the outset to embrace these new technologies.

Vehicle technologies and its privacy implications

Recent technology developments are changing the vehicle market around the world. By 2020, it is expected that 75% of the estimated 92 million cars shipped globally around the world will be built with internet hardware technology.¹

Vehicle technology can be classified in different categories. Each of them collects and uses data regarding vehicle operations and vehicle occupants:

Event Data Recorders (EDR):

It is also known as the "Black Box" in vehicles.² EDRs are devices capable of recording events, such as car crashes. EDRs also can collect information about occupants of vehicles, for example, the use of seat belts.

¹Greenough, John 'Connecting cars to the Internet has created a massive business opportunity' published in the Business Insider Australia on 28 May 2015, < <http://www.businessinsider.com.au/connected-car-market-forecast-report-2015-5>>



On-Board Diagnostics (OBD):

They are not new and have been built into vehicles since the 1990s.³ They were designed to monitor the performance of some of the engine's major components. The system also provides owners with early warnings of malfunctions.⁴

Insurance companies use access to OBD data to customise their policies and personalise insurance rates, with driver permission.⁵ In order to do this, insurance companies provide drivers with devices (OBD-II) in order to continually collect information about how the vehicle is driven.⁶ In the United States there are already State insurance laws regulating these sorts of technologies offerings.⁷

Connected Cars:

The term connected cars refers to vehicles connected over the internet or via 'Dedicated Short-Range Communications' (DSRC).⁸

Intelligent car or driverless cars:

It refers to automobiles operated without human assistance.⁹

Some of the prominent features of these technologies have the potential to collect data including:

- Location of car and diagnostic information to assist in emergency response. This enables drivers to receive location-based warnings and information about weather emergencies and road conditions. This information also allows manufacturers to get feedback about how vehicles are performing.¹⁰
- Behavioural information can also be collected. Vehicle technologies can gather information about the driver's attention, speed, steering and breaking habits. This information can be combined with other diagnostic data to provide new safety features.¹¹

² Duisberg, Alexander, *Connected Cars: A Global Challenge*, (12 May 2015), Pg 2

<<http://www.law360.com/articles/650332/connected-cars-a-global-privacy-challenge>>.

³ Future of Privacy Forum, 'The Connected Car and Privacy Navigating New Data Issues' ("Privacy Forum") (13 November 2014) Pg 3 <<https://fpf.org/2014/11/13/new-fpf-paper-the-connected-car-and-privacy-navigating-new-data-issues/>>

⁴ Privacy Form, Pg 4

⁵ Ibid

⁶ Ibid

⁷ Ibid

⁸ Ibid Pg 5

⁹ Concept extracted from Thierer, Adam & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 Wake Forest J. L. & Pol'y 339 2015, Pages 344-345

¹⁰ Privacy Forum 6

¹¹ Ibid.



- The use of these technologies also require the need to activate on-going user accounts, therefore information such as names, address, billing information etc. is also collected.¹²
- In the near future, cars will be able to collect biometric information such as facial recognition, vital signs, voice samples, health information (pulse).¹³

Vehicle to Vehicle communication (v2v) and vehicle to Infrastructure (v2I):

This technology allows vehicles to 'talk' to each other (v2v).¹⁴ It also allows vehicles to share information with other intelligent infrastructure (v2I) such as a communication network.¹⁵ This means that cars can be connected to a network that allows each vehicle connected to know the position, speed, and direction of every nearby car.¹⁶

Privacy implications

Vehicles have now the potential to collect and transmit an unlimited volume of data regarding behavioural, geographical, even biometrical information relating to drivers. This means that holders of this type of information need to be careful and think about how to comply with privacy laws. For example, an organisation in NSW holding data from vehicles capable of identifying the health condition of a driver will be subject to the provisions and health privacy principles under the *Health Records and Information Privacy Act* (HRIP Act)¹⁷. Therefore, organisations holding this type of information would have the obligation to comply with data retention and data protection principles.¹⁸ This means, that even small players need to have security safeguards that are reasonable to protect the data against loss, unauthorised access, use etc.¹⁹

It is yet too early to predict what effect these new technologies may bring to the safety of drivers. However, it is important to note that some concerns have been raised in relation to

¹² Ibid, Pg7

¹³ White, Joseph "Eyes on the road, A car that takes your pulse" The Wall Street Journal 2012 & Future of Privacy Forum, 'The Connected Car and Privacy Navigating New Data Issues'(13 November 2014) , <https://fpf.org/2014/11/13/new-fpf-paper-the-connected-car-and-privacy-navigating-new-data-issues/>

¹⁴ Concept extracted from Thierier, Adam & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 Wake Forest J. L. & Pol'y 339 2015, Pg 345.

¹⁵ Privacy Forum, Pg 10

¹⁶ Ibid

¹⁷ See definition of health information under section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act).

¹⁸ HRIP Act Sch 1 sec 5

¹⁹ Ibid.

the safety of connected cars when poorly written software make them vulnerable to cyberattacks which may render the car unstable or dangerous for drivers.²⁰

What can be done with the data also poses privacy implications, for example, data collected from vehicles may potentially be disclosed to law enforcement agencies for law enforcement purposes.²¹ While this can be beneficial from a law enforcement perspective, it can be equally intrusive on individuals' privacy.

Lastly, privacy and data protection regulation may not always be adequate and could potentially face challenges. In other countries such as Germany, France, Austria, Italy, Spain, and United of Kingdom the question of data ownership produced by EDR devices is still unclear.²²

Privacy by Design

"Privacy by Design" (PbD) is a concept developed in 1990s in Ontario, Canada.²³ PbD is a principles based approach that encourages organisations and entities to implement privacy as a default mode of operation in their systems and practices and not only as a mere legal compliance requirement.²⁴

PbD has seven corollary principles that can be applied to any type of information, especially sensitive data. The principles include²⁵

1. Proactive not reactive: to favour the implementation of proactive measures as opposite to reactive measures.
2. Privacy as the default system: privacy is built in into systems and practices from the outset.
3. Privacy embedded into the system: as privacy is embedded into the design of business practices and systems, therefore privacy becomes part of the system.
4. Full functionality: PbD accommodates other legitimate interest and objectives so it can make trade-offs when necessary.

²⁰ International Data Corporation, Duncan Brown, 'Responsibility for Vehicle Security and Driver Privacy in the Age of the Connected Car' IDC#EMEA41026016 <<http://www.veracode.com/sites/default/files/Resources/Whitepapers/idc-veracode-connected-car-research-whitepaper.pdf>>

²¹ For example, see exemption under HRIP Act Sch 1 sec 11 (j)

²² Duisberg, Alexander, *Connected Cars: A Global Challenge*, (12 May 2015)
<<http://www.law360.com/articles/650332/connected-cars-a-global-privacy-challenge>>.

²³ Concept developed by Ms Ann Cavoikian, the then Information and Privacy Commissioner of Ontario, Information and Privacy Commissioner of Ontario, Cavoukian, Ann, 'Privacy by Design' the 7 Foundational Principles' Published on August 2009 <<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundatio>>

²⁴ Ibid & Information and Privacy Commissioner of Ontario, Cavoukian, Ann, 'Privacy by Design' the 7 Foundational Principles, *Implementation and Mapping of Fair Information Processes*'

²⁵ Ibid

5. End-to End Security: as privacy is embedded into the system, data is securely protected throughout its entire lifecycle.
6. Visibility and Transparency: means implementation of fair information practices.
7. Respect for User Privacy: PbD focus on the interests and needs of individual users and empower them to play an active role in managing their data.

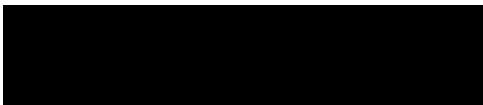
These principles for instance can be implemented to embrace new vehicle technologies and its privacy implications by organisations concerned with new vehicle technology.

I consider that, since this enquiry is concerned with new vehicle technologies and the impact upon the training and education of new drivers and experienced drivers, it is significant to highlight the possible privacy implications these new technologies could bring to drivers in NSW and the approach organisation may take to embrace these new technologies, such as the implementation of 'Privacy by Design'.

I am happy to assist the Standing Committee further with any questions raised by this submission.

I agree to this submission being published, should the Committee decide to publish submissions. Please ensure that prior to the publication of this letter that my signature is redacted from the version to the published.

Yours sincerely



Dr Elizabeth Coombs
A/ NSW Privacy Commissioner

8/12/2016