The Information Commissioner's response to the House of Lords Select Committee on Science and Technology's call for evidence on autonomous vehicles

Introduction

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

2. The Commissioner welcomes the opportunity to respond to the House of Lords Select Committee on Science and Technology's call for evidence on autonomous vehicles. The response addresses those questions posed by the Committee which are relevant to the work of the Commissioner.

What are the potential user benefits and disadvantages from the deployment of autonomous vehicles?

3. While autonomous vehicle technology has the potential to deliver societal benefits in terms of improved road safety and user convenience, there is a need to consider the volume and nature of the data that vehicles may generate and to adopt appropriate safeguards against misuse of individuals' data.

4. Information generated by connected and autonomous vehicles is likely to contain personal data, which should be processed in accordance with the requirements of the DPA, including the eight data protection principles (see annex). Personal data processed via connected and autonomous systems may include geolocation data, telematics, driver/user settings and collision information. There is

also potential for data which may initially be regarded as purely technical in nature, such as safety system information on the number of persons occupying a vehicle, to become personal data if it can be linked to a particular individual or individuals. Data may be stored by on-board systems, transmitted to the vehicle manufacturer or, in the case of autonomous vehicles, used to communicate with other vehicles and traffic management systems.

5. If the personal data of vehicle drivers and users is processed inappropriately, in the case of geolocation data for example, there is a heightened risk of intrusion into individuals' work and private lives. The Government and technology providers should therefore adopt a privacy by design approach and ensure that privacy protections are built in to the design and development of new products and services, thereby reducing the need for costly reworking at a later stage.

6. A privacy by design approach, including the use of privacy impact assessments, can help to reduce the risk of personal data being processed in a manner which breaches the requirements of the DPA and causes detriment to individuals. Mitigating the potential privacy risks at an early stage of development will help to ensure that individuals are able to benefit from connected and autonomous vehicle technology with minimal disadvantage.

7. Technology providers and vehicle manufacturers should seek to create transparency around the types of personal data processed by connected and autonomous vehicle technology and the purposes of the processing. A transparent approach will not only help to satisfy the fairness requirements of the first data protection principle but can also assist in generating consumer trust around the technology.

How much is known about public attitudes to autonomous vehicles?

8. The Information Commissioner's Office (ICO) plans to issue its own call for evidence on connected and autonomous vehicles in order to develop understanding of public attitudes towards the technology and gather information on the steps technology providers and

vehicle manufacturers are taking to address privacy and data protection concerns.

9. In November 2015, the Federation Internationale de l'Automobile (FIA) Region 1 published the results of a public survey on connected cars, which provided an indication of the public's main concerns in relation to connectivity[1]. Respondents to the survey were most concerned about disclosures of private information (88%), followed by commercial use of personal data (86%), vehicle hacking (85%) and location tracking (70%).

10. While the FIA Region 1 survey focused on attitudes towards the types of connected vehicle technology already available on the market, the results suggest that the public's main concerns all relate to privacy issues, which may act as a useful indicator of the concerns likely to arise as autonomous vehicle technology develops.

Does the Government have an effective approach on data and cybersecurity in this sector?

11. The Government is yet to address the challenges related to data and cybersecurity in this sector directly with the ICO. However, the establishment of the Centre for Connected and Autonomous Vehicles (CCAV) is a welcome development. CCAV should seek to place privacy, data protection and cybersecurity considerations at the heart of its work to develop policy in the sector.

12. As noted above, personal data generated by connected and autonomous vehicle technology should be processed in accordance with the DPA and the eight data protection principles. In developing policy around cybersecurity and the processing of personal data in the sector, the Government should refer to the requirements of the seventh data protection principle (see annex).

13. The ICO supports the Government's Cyber Essentials scheme and has encouraged businesses to be assessed against it. As a minimum, the Government should seek to apply the standards and principles promoted through the scheme to the connected and autonomous vehicles sector, recognising the high level of risk

[1] http://www.fia.com/news/fia-reveals-what-data-being-tracked-and-how-public-reacts-connected-cars

associated with potential cyber-attacks on internet connected vehicles.

Additional information

14. The ICO has undertaken some initial work with representative bodies for vehicle manufacturers and fleet management companies in order to develop its understanding of the data protection and privacy risks arising from the deployment of connected and autonomous vehicle technology. The ICO is keen to work with industry and policy makers to help address any challenges at an early stage.

15. It should be noted that data protection law across Europe is due to undergo significant reform when the General Data Protection Regulation comes into force in May 2018. The Regulation will update data protection law to take into account technological developments and globalisation, and reflects the fact that technology allows organisations to make use of personal data on an unprecedented scale. It will be important to ensure any work undertaken in relation to connected and autonomous vehicles takes into account the new data protection framework.

16. The ICO would welcome the opportunity to engage with the Government, the Department for Transport and CCAV to help ensure the issues identified are adequately addressed.

October 2016

Annex

Data Protection Act 1998

The data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.