International Working Group
on Data Protection
in Telecommunications

Connected Vehicles

63rd meeting, 9-10 April 2018, Budapest, HUNGARY

Introduction

1. In 2011, the Working Group adopted a Working Paper on Event Data Recorders (EDR) in Vehicles.[1] Since that time, there has been considerable further technological development regarding the processing of data – including personal data – in, between as well as outside vehicles. Connected vehicles are complex Internet of Things (IoT) systems on wheels, consisting of many electronic control units (ECU) that are linked together via an in-vehicle network.

2. As of today, many vehicles are still not natively connected. Technologies are being developed and applied to allow for communication via mediating entities or directly between vehicles or road infrastructural facilities (e.g., traffic signs or transmitting/receiving base stations) without the intervention of a network operator.

3. Envisaged applications for connected vehicles are diverse and can be classified as:[2]

    a. *Mobility management*: functions that allow drivers to reach a destination quickly, and in a cost-efficient manner, by providing timely information about potentially dangerous environmental conditions (e.g., icy roads), traffic congestion or road construction work, parking lot or garage assistance, optimised fuel consumption or road pricing.[3]

    b. *Vehicle management*: functions that aid drivers in reducing operating costs and improving ease of use, such as notification of vehicle condition and service reminders, transfer of usage data (e.g., for vehicle repair services), customised “pay as/how you drive” insurances, remote operations (e.g., heating system) or profile configurations (e.g., seat position).

---

1 IWGDPT Working Paper: Event Data Recorders (EDR) on Vehicles / Privacy and data protection issues for governments and manufacturers (Montreal, Canada 4-5 April 2011), https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2011/2011-WP-EDR_on_vehicles.pdf

2 PwC Strategy 2014. "In the fast lane. The bright future of connected cars", https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

3 IWGDPT Report and Guidance on Road Pricing – “Sofia Memorandum” – (Sofia (Bulgaria), 12./13.03.2009), https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2009/2009-Sofia_Memorandum-en.pdf

c. *Road safety*: functions that warn the driver of external hazards and internal responses of the vehicle to hazards, such as collision protection, hazard warnings, lane departure warnings, emergency call (*eCall*), or crash investigation "black-boxes".

d. *Entertainment*: functions providing information to and involving the entertainment of the driver and passengers, such as smart phone interfaces, WLAN hot spots, music, video, Internet, social media, mobile office or "smart home" services.

e. *Driver assistance*: functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways.

f. *Well-being*: functions monitoring the driver's comfort, ability and fitness to drive such as fatigue detection or medical assistance.

4. As vehicles become increasingly connected to the Internet and to other vehicles, more and more personal data will be collected and processed by the vehicles and will become accessible to third parties. Relevant types of data collected by the vehicle's sensors may concern driver behaviour or information about other people inside or outside the vehicle. This data may be processed by the vehicle's IT systems, or when other personal devices connect to it.[4] The advent of autonomous vehicles will raise additional privacy issues, as their functioning will require the collection and use of significant amounts of data, some of which will be personal data.

Current and Emerging Stakeholders

5. Telematics and other driver related data may be available to a range of companies, from vehicle manufacturers, servicing companies, rental and car sharing companies, motor insurance companies and entertainment providers.

6. Furthermore, a telematics services industry for vehicles has emerged which also processes personal data in connection with the use of vehicles.[5] New business models have arisen such as those developed by insurance companies (e.g., "pay as/how you drive"), which rely heavily on the processing of drivers' personal data.

7. Fleet managers, leasing companies and employers providing vehicles to members of their staff also share an interest within the collection of personal data produced by connected vehicles (e.g., in order to allocate resources, track vehicles or bill services).

---

[4] Infographic "Data and the connected car" by the Future of Privacy Forum, https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

[5] Testimony and Statement for the Record of Khaliah Barnes, Associate Director and Administrative Law Counsel, EPIC, at the Hearing on "The Internet of Cars", Joint Hearing before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittee on Information Technology and Subcommittee on Transportation and Public Assets, November 18, 2015, https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf

8. Finally significant amounts of data will be collected by developers of autonomous vehicles (or components thereof) for the purposes of the design of their products. The advent of autonomous vehicles will raise additional privacy issues as their development, operation and maintenance will result in the processing of large amounts of data, some of which will be personal data, by, among others, developers and makers of such vehicles.

9. New actors, especially those coming from the Internet industry, may apply their current practices for storing and processing personal data (i.e., storing and processing data not related to the primary purpose of the data collection) to the automotive industry.[6]

Scope of this document

10. This document addresses privacy risks arising from the collection and processing of data in different contexts and by different systems:

    a. Data collected and processed by the vehicle, including information and entertainment systems built into the vehicle.

    b. Data exchanged between the vehicle and personal devices connected to it,

    c. Data exchanged between the vehicle and external entities (e.g., infrastructure managers, vehicle manufacturers, insurance companies, car repairers).

    d. Data broadcast to surrounding vehicles and infrastructure entities to enable Cooperative Intelligent Transportation Systems (C-ITS).[7]

11. Vehicle manufacturers, among other stakeholders, collect and process data to design autonomous vehicles that are a particular type of connected vehicle. This document will discuss the collection of data for and by autonomous vehicles but will not discuss the more general ethical questions raised by the deployment of autonomous vehicles. In addition, the collection and processing of data by autonomous vehicles and the associated restrictions such as the need for real time processing is out of scope of this paper.

12. Some of the data collected within or by connected vehicles are used to improve public safety and reduce the number of accidents. For instance, low latency vehicle-to-vehicle communications may help to quickly trigger a driver's reaction to a developing traffic incident. This opinion does not attempt to find a compromise between privacy and public safety but instead provides recommendations to improve privacy while still allowing the use of data for the specified purposes.

---

[6] For instance, the "Open Automotive Alliance" (OAA), a global alliance of the major technology and car industry companies, aims at using the Android platform in automobiles, http://www.openautoalliance.net

[7] Cooperative Intelligent Transport Systems (C-ITS) use technologies that allow road vehicles to communicate with other vehicles, with traffic signals and roadside infrastructure as well as with other road users. The systems are also known as vehicle-to-vehicle (V2V) communications, or vehicle-to-infrastructure (V2I) communications.

13. Employers providing company cars to members of their staff might want to monitor their employee's actions (e.g., in order to ensure the safety of the employee, goods or vehicles, to allocate resources, to track and bill a service or to check working time). Access to the data generated by connected cars in this context is out of scope of this paper.

Types of data considered

14. Different types of data can be collected, generated, transmitted, processed or retained by connected vehicles. Some of these data, such as owner/driver data, identifiers (e.g., vehicle identification numbers, MAC addresses) or location data can be directly associated with a specific device or a natural person. Besides, advanced functionalities might allow the processing of biometric data for the authentication of the driver (e.g., voice-, fingerprint-, video- and other types of authentication) or his monitoring (e.g., image processing for fatigue detection).

15. Other data are indirectly linked to the driver such as telematics data (e.g., speed, accelerations, application of brakes, seat occupation, and shock detection) or servicing data. They may also be linked to the driver or other occupants of the car (e.g., alcohol presence, items held or used, identification of passengers' actions, or other behaviour-related data, etc.). Some of those data will also be personal data.

Existing and emerging regulations, obligations and recommendations

16. Connected vehicles have become a substantial subject for regulators over the last decade, with a major increase in the past two years. Those regulations and initiatives complement the existing data protection and privacy frameworks.

17. The development of connected vehicles and in particular Cooperative Intelligent Transportation Systems (C-ITS) is being fostered by national governments as well as by supranational actors:

    a. In 2014, the European Commission set up a platform for the deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform) to create technical infrastructures and standards for communication between vehicles and between vehicles and roadside elements.[8]

    b. In 2016, member states and the Commission launched the C-Roads Platform to link C-ITS deployment activities, jointly develop and share technical specifications and to verify interoperability through cross-site testing.[9] Many C-Roads pilots have been initiated such as "NordicWay Coop" to test a pre-deployment of C-ITS services in four countries (Finland, Sweden, Norway and Denmark).

---

[8] European Commission, Mobility and Transport, http://ec.europa.eu/transport/themes/its/c-its_en.htm

[9] C-Roads, https://www.c-roads.eu/platform.html

18. In January 2016, the Conference of the German Federal and State Data Protection Authorities and the German Association of the Automotive Industry (VDA) published a common declaration on the principles of data protection in connected and not-connected vehicles.[10]

19. In January 2017, the European Union Agency for Network and Information Security (ENISA) published a study focused on cyber security and resilience of smart cars listing the sensitive assets present in smart cars, as well as the corresponding threats, risks, mitigation factors and possible security measures to implement.[11]

20. In August 2017, the UK Centre for Connected and Autonomous Vehicles (CCAV) released a guide stating principles of cyber security for connected and automated vehicles in order to raise awareness on the matter within the automotive sector.[12]

21. In September 2017, the International Conference of Data Protection and Privacy Commissioners adopted a resolution on connected vehicles.[13]

22. In 2017, the U.S. House of Representatives passed H.B. 3388, the Safely Ensuring Lives Future Development and Research in Vehicle Development (SELF DRIVE) Act to encourage the testing, development and deployment of highly automated vehicles ("HAVs") in the United States, which includes privacy and cybersecurity provisions.[14] The Federal Trade Commission released a staff perspective on its 2017 workshop on connected vehicles[15] while the U.S. National Highway Traffic Safety Administration released the paper "Automated Driving Systems 2.0: A Vision for Safety," which provides voluntary guidance that intends to encourage best practices and prioritizes safety.[16]

---

[10] Data protection aspects of using connected and non-connected vehicles, https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf

[11] Cyber security and resilience of smart cars, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[12] Principles of cyber security for connected and automated vehicles, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[13] Resolution on data protection in automated and connected vehicles, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf

[14] H.R.3388 - SELF DRIVE Act, https://www.congress.gov/bill/115th-congress/house-bill/3388

[15] Staff Perspective Recaps Workshop Examining Privacy, Security Issues Related to Connected Cars, https://www.ftc.gov/news-events/press-releases/2018/01/staff-perspective-recaps-workshop-examining-privacy-security

[16] Automated Driving Systems 2.0: A Vision for Safety, https://www.nhtsa.gov/manufacturers/automated-driving-systems and https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

23. In October 2017, the Article 29 Working Party adopted an opinion on the processing of personal data in the context of Cooperative Intelligent Transportation Systems (C-ITS).[17]

24. In October 2017, the French data protection authority (CNIL) released a compliance package for connected cars. These guidelines provide assistance to stakeholders on how to integrate data protection by design and by default, enabling data subjects to have effective control over their data.[18]

25. In some jurisdictions, the capability for vehicles to connect to existing telecommunications networks is now mandatory (e.g., in the European Union, vehicles manufactured after March 2018 are required to include the so-called "*eCall*" System).[19]

Privacy risks

26. Data subjects have data protection rights concerning the processing of data related to them, within the limits prescribed in applicable law. This right is inalienable and not transferable. The discussion about ownership of vehicle data might mislead controllers into denying data subjects their rights.[20,21]

Lack of transparency

27. Vehicle drivers and passengers may not be adequately informed about the processing of data taking place in or through a vehicle. The information may be given only to the vehicle owner, who may not be the driver, and may also not be provided in a timely fashion (i.e., before a vehicle is purchased, rented or used).

---

[17] Article 29 Working Party, WP252, Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888

[18] Compliance package for a responsible use of data in connected cars, https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data

[19] *Ecall* is intended to facilitate the provision of rapid assistance to motorists involved in an accident in member states of the European Union, cf. https://en.wikipedia.org/wiki/ECall. For a discussion of the related privacy issues see e.g. Article 29 Working Party: Working document on data protection and privacy implications in *eCall* initiative, Adopted on 6th September 2006 (WP 125), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp125_en.pdf and Opinion of the EDPS on the proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the *eCall* system and amending Directive 2007/46/EC, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-10-29_eCall_EN.pdf

[20] ACEA position paper – Access to vehicle data for third party services, http://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf

[21] Fair and equal access to vehicles in a digital single market, https://www.figiefa.eu/wp-content/uploads/Manifesto-for-Fair-Access-to-the-Vehicle.pdf

28. Sensor technology (e.g., proximity testing, camera) in vehicles may not only be used for observation of drivers and passengers inside the vehicle, but also for monitoring the area surrounding the vehicle. People may not be aware of this data collection, and informing them will be difficult to achieve.

Unlawful processing

29. In order to process personal data using vehicle IT systems, a data controller needs a legal basis. Depending on the purpose of the data processing, various legal grounds can be used (consent, performance of a contract, legitimate interest…). A risk exists that controllers may not meet this requirement, and engage in unlawful processing.

Unauthorized secondary use

30. Data collected by vehicle manufacturers, service providers or any other third party might be used or sold for unconsented purposes. An example of such an unconsented purpose would be the analysis of driving behaviour by motor insurance companies outside of the performance of a particular insurance contract.

31. In Cooperative Intelligent Transportation Systems (C-ITS) messages sent from vehicle to vehicle or from vehicle to infrastructure entities are meant to be broadcasted and therefore are not secured against unauthorized third party access. They may be intercepted by anyone present in the range of the signal, and could be used to set up location profiles of vehicles and their drivers.[22]

32. Data collected by connected vehicles could be used by law enforcement to detect speeding or other infractions, or for surveillance, unless specifically foreseen by law.[23]

Excessive collection

33. Numerous sensors being deployed in connected vehicles there is a very high risk of excessive data collection compared to what is necessary to achieve the purpose. This is in particular the case if the sensors and the IT systems attached to them are not designed with data protection by design principles in mind, such as purpose specification and data minimization.

---

[22] Note that even the use of privacy friendly technologies – in this case rapidly changing pseudonyms – may not prevent location profiling, http://spectrum.ieee.org/cars-that-think/transportation/advanced-cars/researchers-prove-connected-cars-can-be-tracked

[23] In the EU, such data will be considered special categories of data. The processing of such data is prohibited, unless one of the specific legal exceptions applies (Art. 9 GDPR).

34. Connected vehicles offer wireless connection capabilities to allow drivers and passengers to share content with the vehicle. This may result in an excessive amount of data being collected from smart phones, telematics smart boxes and other personal devices of passengers.

35. The development of autonomous vehicles, and more specifically of machine learning algorithms, may require a large amount of data collected over a long period of time.

Lack of control

36. There is a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights.

37. During their lifetime, vehicles may belong to more than one owner either because they are sold or because they are being leased rather than purchased. In addition, vehicles are increasingly being shared or rented, not just by companies, but also individuals. Yet, it is currently not possible, or very difficult to erase or back up the data. There is a risk that data relating to previous occupants of the vehicle are visible to subsequent users.

38. Rental vehicles, leased vehicles and taxis (that are not necessarily owned by the driver) are likely to collect data of drivers and passengers that do not relate to the vehicle's owner. This includes employees that use a leased car issued by their employer. In such circumstances, the person whose data is collected may not be able to object to some data processing.[24]

Inadequate security

39. The plurality of functionalities (e.g., entertainment, smart phones) and interfaces (e.g., web, USB, RFID, Wi-Fi) offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised.

40. Unlike most Internet of Things devices, connected vehicles are critical systems where a security breach may endanger the life of its users and people around. The importance of addressing the risk of hackers attempting to exploit connected vehicles' vulnerabilities is thus heightened.

41. Personal data stored on vehicles and/or at external locations (e.g., in cloud computing applications) may not be adequately secured against unauthorized access. For instance, during maintenance, a vehicle has to be handed to a technician who will require access to some of the vehicle technical data. While the technician needs to have access to the technical data, he could abuse his capabilities to access all the data stored in the vehicle. In addition, vehicle data

[24] Connected cars: What Happened to Our Data on Rental Cars, https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf

represents an asset that may not be appropriately secured by companies whose historical core business has not been related to personal data processing.

42. Driver assistance functions can lead connected vehicles to take decisions, for instance in advising the driver to change lanes or using cruise control. In case of inaccuracy of data, such decisions could have disastrous consequences in terms of road safety.

43. Connected vehicles require very low response time to ensure vehicles react in a timely manner in an emergency (e.g., when the driver is avoiding a collision). Hackers could exercise serious impacts on the driving system responsiveness by exploiting system malfunctions and by consuming large amounts of CPU resources and bus bandwidth.

Lack of accountability

44. Vehicle manufacturers, component manufacturers and software developers may collect different types of data for different purposes. Some may be data controllers; some may be data processors and there is a risk of poor and/or non-transparent allocation of roles and responsibilities between joint data controllers and processors.

45. Vehicle data is often perceived as being non-personal data because it may not be possible to directly link this data to the identity of the data subjects. Not all data collected or emitted by vehicles are personal data, but, for instance, data specifying the location of a vehicle at multiple points in time can very often be linked to a specific person. Entities processing vehicle data may fail to assess whether or not they are processing personal data, and could end-up processing personal data in contravention of applicable legislation.

Recommendations

Vehicle and equipment manufacturers

46. Information about the scope, the purposes, the controllers of the processing and data subjects rights should be easily accessible (e.g., through the dashboard). If information about passengers is also collected (e.g., by on-board sensors), they should also be informed appropriately. For example, if a vehicle is always listening for a triggering phrase, the vehicles should have a clear signal on-board (such as a light) to inform passengers about the data collection inside the vehicles. To be complete, information given to driver and passengers should list the rights of the person (e.g., their rights to access, their right to object, to withdraw consent and the right to data portability) in jurisdictions where such rights exist.

47. Vehicle sensor systems should avoid storing personal data of persons that are outside the vehicle. In addition, if data is stored and not immediately deleted after real time processing, faces and vehicle plates collected by vehicle cameras should be detected and permanently blurred.

48. A profile manager implemented inside the vehicle could store the preferences of known drivers to allow them – and to some extent frequent passengers such as family members – to adapt and record their privacy settings. This would significantly reduce the time required for repeated changes to the settings.

49. Some of the functionality provided by connected vehicles, and their associated data processing, only requires connectivity with other on-board components (e.g., a smart phone connected to the vehicle). Vehicle and equipment manufacturers should prioritize communications within the vehicle and avoid transmitting data to remote servers when that is not strictly necessary.

50. Vehicle systems required for core critical functions related to driving should be isolated from systems supporting optional features like entertainment in order to ensure that the vehicle will still function properly if a non-critical system shuts down or behaves improperly.

51. In the absence of specific legislation, drivers should still have the ability to halt the collection of certain types of data temporarily or permanently, provided that such data is not essential to the critical functions of the vehicle (e.g., the driving system).

52. In addition to configuring privacy by design and by default settings, manufacturers should facilitate data subjects' control over their data during the entire processing period. Specifically, that control should extend to all configurations that have an impact on privacy, in particular:

    a. The option to easily modify those configurations, during the entire processing period, especially for the purpose of activating or deactivating services based on consent or on the performance of a contract (e.g., commercial offers personalised on the basis of geolocation, breakdown assistance).

    b. Where appropriate, the option to adjust the level of detail of the data collected to the level of service requested (e.g., accessing a map without being geolocated if they do not wish to be guided).

    c. The option to easily exercise their rights including access and, if appropriate, deletion.

53. Geolocation data are particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they enable the places of work and of residence to be deduced, as well as the driver's centres of interest (e.g., leisure, possibly religion through the place of worship, or sexual orientation through the places visited). Accordingly, the service provider should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing.

54. Cooperative Intelligent Transportation System (C-ITS) should limit the communication of personal data to the necessary recipients. For instance, data that is only useful in a vehicle-to-vehicle communication context should not be

collected and stored by infrastructure managers or by vehicle and equipment manufacturers when this data is not processed for a clearly identified purpose.

55. The personal data of vehicle drivers, passengers or vehicle owners may be stored by different parts of the system, each supporting different functionality (e.g., by the phone book of the vehicle, the sound system, and the navigation system). Wiping personal data from the vehicle may, therefore, require multiple operations. Manufacturers should centralize the functionality needed to facilitate the deletion of personal data in order to simplify the removal of personal data from vehicle systems by vehicle resellers and vehicle rental agencies.[25]

56. Where vehicle and equipment manufacturers act as data controllers that employ other parties, either as joint controllers or as data processors (such as added-value service providers, smart phone integration and application providers), they should clearly allocate their respective roles, responsibilities and rights regarding the processing of personal data. If the third party acts as a data processor, the agreements should stipulate that it may only process personal data in accordance with the instructions of the data controller. Due consideration should also be given to other legal requirements regulating contractual processing of personal data.

57. Vehicle and equipment manufacturers should minimize and aggregate data as soon as possible after the specified purposes have been fulfilled. In addition, in order to implement risk-based measures for protecting data security and mitigate the consequences of an unauthorized access, pseudonymisation techniques should be applied.

58. Vehicle and equipment manufacturers as well as service providers must not use the collected data for a purpose that is incompatible with the original purpose, not authorized by law, or for which the data subjects have not given explicit, specific, informed, unambiguous, and freely-given consent.

59. For any subsequent reuse of data collected by connected vehicles inconsistent with the primary purpose, it is necessary to obtain consent and ensure that the use is in line with with expectations of data subjects.

60. It is, however, permissible to process the products of data processing activities which yield anonymized data for other purposes. By definition, anonymized data cannot be directly or indirectly associated with a natural person. Hence, data protection legislation does not apply.

Third party service and applications providers

61. Service and applications providers should embed privacy settings to limit the collection and use of personal data. Individuals should be presented with choices for collection and use of personal data, particularly for non-core functionality, combined with just-in-time notices when the individual is interacting with a feature or service that requires collection and use of personal data. Privacy by design could, for instance, be implemented by processing some data in the vehicle in

[25] Personal Data In Your Car, https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf

order to limit the volume of data that are processed outside of the vehicle. This type of implementation could also reduce bandwidth consumption and speed up data processing.

62. Application providers and third party developers may not have access to all the interfaces that are available to inform the vehicle driver and passenger of their data collection. They should not collect or process data until they can confirm that the driver and passengers are aware of and have consented to the data processing, or that they have another legitimate basis for processing.

Standardization bodies

63. Standards should be created that enable data controllers to comply with their security obligations and in particular to guarantee the confidentiality of the collected data. In the context of connected vehicles, the need for data confidentiality and security shall apply to data collected and processed within the vehicle as well as to data transmitted away from the vehicle. Therefore strong privacy and security standards should be implemented, appropriately adapted to the risks posed by the data processing.

64. Standards for the implementation of the Cooperative Intelligent Transportation Systems (C-ITS) should limit the diffusion of information only to vehicles and infrastructure entities within close range of the emitting vehicle.

65. Standards regulating access to in-vehicle data should facilitate compliance with the applicable legislation and enable data subjects to efficiently exercise their rights.[26]

Drivers

66. When they are adequately informed, vehicle owners should in turn inform other users of the vehicle about data collection and use policies and where possible about the options to choose specific privacy settings. A pre-requisite for the information of passengers is that the driver is himself aware of these data collection and use policies.

Public Authorities

67. Public authorities should mainly use data provided by connected vehicles for purposes that the data subjects have freely consented to or that are in the public interest, or to fulfil tasks that have been laid down in an appropriate law. In order to reduce function creep and facilitate connected vehicle adoption, public authorities should only use these data to adapt the infrastructures, improve road safety and reduce traffic congestion.

---

[26] Access to In-vehicle Data and Resources, https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf

68. Repurposing vehicle data to observe infractions such as speeding or for surveillance purposes must have a clear legal basis.

Rulemaking authorities

69. Rulemaking authorities should make the provision of a function for erasure of personal data (to be applied prior to the sale or next rental of a vehicle) mandatory.

70. Connected vehicles being complex systems should be subject to a Privacy Impact Assessment prior to their release. This requirement should be established through relevant legislation, regulation or policy.