Contribution ID: 250d7824-04c1-4f1f-a536-2232aea1957e
Date: 04/12/2018 23:14:44

Open Public Consultation for building trust in Connected and Automated Mobility (CAM)

Fields marked with * are mandatory.

Background information

Cars and other vehicles are increasingly equipped with sensors, driver assistance systems, Internet connectivity, etc., allowing them to become connected, smart and autonomous. These cars exchange information with other similar cars, the road infrastructure, or with remote data bases, with the aim to provide new mobility services. Fully autonomous vehicles are just around the corner. Building on the previous initiative 'Europe on the Move' of May 2017, on the 17th of May 2018 the European Commission put forward a strategy to make Europe a world leader for automated and connected mobility. The objective is to allow all Europeans to benefit from safer traffic, less polluting vehicles and more advanced technological solutions, while supporting the competitiveness of the EU industry. The strategy looks at a new level of cooperation between road users, which could potentially bring enormous benefits for the mobility system as a whole. Transport will be safer, cleaner, cheaper and more accessible to the elderly and to people with reduced mobility.

The Communication on Connected and Automated Mobility (CAM) proposed a comprehensive EU approach towards connected and automated mobility, setting out a clear, forward looking and ambitious European agenda. This agenda provides a common vision and proposed supporting actions for developing and deploying key technologies, services and infrastructure. Among these actions, it is envisaged that the Commission will work towards the adoption of a Recommendation to be addressed to the Member States and industry actors. The Recommendation would pertain to the use of pioneer spectrum for 5G large-scale testing, cybersecurity issues and into a data governance framework that enables data sharing, in line with the initiatives of the 2018 Data Package, and with data protection and privacy legislation. The aim is to ensure that EU legal and policy frameworks are ready to support the deployment of safe connected and automated mobility, while simultaneously addressing societal and environmental concerns which will be decisive for public acceptance. To gather evidence on the existent bottlenecks and risks but also to validate with the stakeholders possible solutions, a public consultation will be launched to involve all relevant actors of the mobility ecosystem, from public authorities to industry stakeholders and end-users.

Objectives of the Public consultation

Building on the three key areas, where clarification appears to be necessary – data, cybersecurity, use of 5G commercial bands -, this public consultation aims to identify from the general public and relevant stakeholders (car manufacturers, connectivity providers, service providers, telecom providers, end-users,

public authorities, health comunity and civil society organisations) which are the main challenges linked to the deployment of connected and automated cars today. It will build on existing knowledge provided by stakeholders, the EU and United Nations Economic Commission for Europe (UNECE). The consultation investigates the cybersecurity threats and trust issues, the data governance aspects (e.g. governance models; principles for car data sharing), privacy and data protection needs, as well as the different aspects of technology needs.

As all categories of respondents have a general interest in this consultation, from citizens to specialised actors of the mobility ecosystem, a first set of questions is addressing the public. The second set of questions is addressed only to specialised actors of the ecosystem, such as car manufacturers, connectivity providers, service providers, telecom providers, end-users, public authorities, civil sociery organisations etc.

Who are you?

*You are replying as

- A. An individual in your personal capacity/ on behalf of an organisation
- B. On behalf of a (your) business/ association of businesses
- C. On behalf of a public authority

Name of your business/organisation

Electronic Privacy Information Center

Email

info@epic.org

Website of your business/organisation

https://epic.org

Please indicate the main place of operation of your business/organisation

United States of America

Please indicate the primary place of establishment of the entity you represent

United States of America

*Please specify your role in relation to connected and automated mobility sector

- Automotive supplier (Tier 1, Tier 2, …)
- Automotive downstream market supplier (aftersales, maintenance, Mobility as a Service)
- Telecom provider
- Original Equipment Manufacturer (OEM)
- Vendor (e.g. of vehicles or vehicle components)
- Insurance company

- ○ Standardisation body
- ◉ Other, e.g. re-user of in-vehicle data outside of the automotive sector, such as data analytics

* If you replied "Other" above, please specify.

800 character(s) maximum

NGO

General questions

* Do you think there should be regulatory measures in place to secure the connected and automated vehicle against cyber-attacks?

- ◉ Yes
- ○ No
- ○ I don't know

* Do you think the car manufacturers should put forward measures to secure the connected and automated vehicle against cyber-attacks?

- ◉ Yes
- ○ No
- ○ I don't know

* Which of the below actions should, in your view, be prioritized to increase cyber-security resilience of connected and automated cars?

- ○ Test before vehicle goes to market
- ○ Certification to increase the security of connected and automated cars (e.g. certification schemes, specific quality labels, etc.) after the cars have been put on the market
- ○ Specific laws to address cyber-security concerns (e.g. introduce specific security measures)
- ○ None of the above
- ◉ Other
- ○ I don’t know

* If you replied "Other" above, please specify.

800 character(s) maximum

Testing vehicles before going to market, Certification to increase the security of connected cars after being put on the market, and specific laws to address cybersecurity concerns should all be prioritized.

* In-vehicle data may disclose information about you (e.g. driving habits, location data) and giving access to these data may result in individuals concerned being subject, amongst others, to differentiating pricing practices, targeted advertising, and alike or even refusal of services. Despite these risks, would you give your consent to access your in-vehicle data to private companies for developing more digital car services, such as parking slots or automotive navigation systems?

- ○ Yes
- ◉ No
- ○ I don't know

* In-vehicle data may disclose information about you (e.g. driving habits, location data). Despite any potential privacy risks associated with the processing of your in-vehicle data, would you still give your consent to access that data to public authorities, e.g. for increasing road safety?

- ( ) Yes
- (•) No
- ( ) I don't know

* Would you agree that other companies than the car manufacturer, get access upon your consent to your in-vehicle data to develop services (e.g. insurance, garage assistance, etc.)?

- ( ) Yes
- (•) No
- ( ) I don't know

* What are your main concerns relating to the use by other companies of your in-vehicle data?

800 character(s) maximum

EPIC recognizes the benefit of using anonymized data for providing safer car features and additional services. However, the GDPR must regulate all uses of personally-identifying information. Individual privacy interests must take priority over non-basic product features.

* Which additional services would you consider important to receive and of need to you when giving access to your connected and automated car data? (You can pick more than one answer)

- [ ] Information on available parking slots
- [ ] Information on road accidents
- [ ] Information on fastest roads and traffic jams
- [ ] Information on fuelling stations
- [x] Other

* If you replied "Other" above, please specify.

800 character(s) maximum

EPIC recognizes the benefit of using anonymized data for providing safer car features and additional services. However, the GDPR must regulate all uses of personally-identifying information. Individual privacy interests must take priority over non-basic product features.

* How important is it for you to be able to choose between different providers of value-added in-vehicle services independent from the car manufacturer (e.g. providers of information about parking slots, audio-visual media content, electronic gaming, etc.)?

- (•) Very important
- ( ) Important
- ( ) Not important at all
- ( ) I don’t know

* Are there other aspects that should be taken into account by the regulators and industry actors when developing connected and automated vehicles and related mobility services that are not covered by this public consultation? Please explain your reply.

800 character(s) maximum

As with all Internet of Things products, connected and automated vehicles present significant safety risks from hacking vulnerabilities and collection of vast amounts of personal data without driver consent. Wireless hacking can occur from anywhere in the world via the Internet, giving hackers access to the driver's physical location using built-in GPS navigation systems, allowing hackers to interfere with vehicle operation while the car is on the road, and providing access to driver's personal information, which can be used for identity theft. These risks must be taken into account when developing standards for connected and automated vehicles.

* You finished the first set of questions. If you have a specific interest in this consultation (you are an end-user, car manufacturer, connectivity provider, service provider, telecom provider, and public authority, etc.), you can continue with the second set of more technical questions. Do you want to continue?

- (●) Yes
- ( ) No

* Are you:

- ( ) End-users (for private and professional consumption)
- (●) Specialised industry actors (e.g. Automotive supplier, Automotive downstream market supplier, Telecom provider, Original Equipment Manufacturer (OEM), Vendor (e.g. of vehicles or vehicle components), Insurance company, Standardisation body, etc.)
- ( ) Public authorities

Cybersecurity

Vehicle connectivity and system integration of thousands of components originating from different sources bring new threats of cyber-attacks such as taking remote control of the vehicle.

At present there is no sector specific approach on cybersecurity. Generic and transversal actions were proposed through the Commission Communication of 13 September 2017 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' which identifies key priority areas for the voluntary EU cybersecurity certification framework for IT components as proposed in the Cybersecurity Act. One of these priorities is linked to security in critical or high-risk applications, which can also be found in connected and automated cars.

The Communication on Connected and Automated Mobility (CAM) also proposes various measures to set a framework for cybersecurity on CAM. In particular, the Commission proposed that protection of vehicles against cyberattacks is dealt with as part of the revised General Safety Regulation, more specifically to include rules currently being developed at international level (United Nations Economic Commission for Europe (UNECE)). It is essential that, where possible, cybersecurity solutions, and in particular those concerning in-vehicle security are agreed upon at a global level rather than by the EU (or any other country or region) on its own. In addition, the Intelligent Transport Systems delegated act will only address trust and security for the exchange of Cooperative Intelligent Transport Systems messages and for Cooperative Intelligent Transport Systems stations.

Recommendations could be also addressed to other actors of the ecosystem for connected and automated mobility (mobile phone and aftermarket products that may be plugged to vehicles, road operators; third party mobility service providers, cloud service providers, etc.). More specifically, not all components (e.g. road side units, data centres for vehicle data) that may be connected to vehicles are subject to clear

cybersecurity rules. A cyberattack targeting one of these elements (the connectivity, the data infrastructure) can bring vulnerabilities in the system and severely impact the safety and the privacy of the passengers and of other citizens.

The aim of this section is to identify the most relevant concerns raised by the industry stakeholders, end-users, national authorities and other stakeholders in order to better tackle the cybersecurity-related challenges affecting the proper functioning of the connected and autonomous vehicles.

* Cybersecurity is essential to the safety of the vehicle ecosystem. Adequate, sector specific cybersecurity safeguards would increase trust and end-users' acceptance in relation to connected and automated mobility.

- ○ I strongly disagree
- ○ I disagree
- ○ I agree
- ◉ I strongly agree
- ○ I don't know/Not applicable in my case

* Which of the below security issues have you experienced so far? (You can pick more than one answer)

- ☑ Issues in contractual arrangements (e.g. responsibilities are not clearly allocated among the various actors of the ecosystem)
- ☑ Issues in relation to non-embedded software (e.g. of smart devices connected to the connected and automated vehicle)
- ☑ Insufficient protection of the communication interfaces (including Internet and Radio) leading to unauthorized access to the car systems
- ☑ Security issues introduced by 3rd parties actors (e.g. actors having access to the data infrastructure)
- ☑ Other
- ☐ I don't know
- ☐ None of the above

* If you replied "Other" above, please specify.

800 character(s) maximum

Other security issues include company misuse of driver data and/or unauthorized disclosure to third parties (e.g. advertisers) without knowledge and consent. Many connected vehicles incorporate social media apps like Facebook, Waze, and Yelp (e.g. BMW's Connected Drive System) which increases the risk of unauthorized exposure of driver data.

* In light of the cybersecurity risks associated with connected and automated mobility, industry actors should consider measures against cyber-attacks targeting the connectivity and/or automation of the vehicle or the data infrastructure of the connected and automated vehicle.

- ◉ Yes
- ○ No
- ○ I don't know

* If you have considered measures, please, specify which ones.

800 character(s) maximum

Navionics should always be separated from Internet-connected entertainment features by firewall. For more information see: https://epic.org/amicus/cahen/

* In light of the cybersecurity risks associated with connected and automated mobility, industry actors should be obliged to introduce "safety by design" measures against cyber-attacks targeting the connectivity and/or automation of the vehicle or the data infrastructure of the connected and automated vehicle.

- (●) Yes
- ( ) No
- ( ) I don't know

* Requirements for cybersecurity pre-market tests should be further enhanced at EU level.

- ( ) I strongly disagree
- ( ) I disagree
- ( ) I agree
- (●) I strongly agree
- ( ) I don't know/Not applicable in my case

* Cybersecurity should be included in the scope of the EU framework establishing (product) liability rules.

- (●) Yes
- ( ) No
- ( ) I don't know

* EU legislation should be further enhanced or developed for which elements of the cybersecurity ecosystem of the connected and automated car. (You can pick more than one answer)

- [ ] The car data infrastructure
- [ ] The communication interfaces
- [ ] Non-embedded software
- [x] All of the above
- [ ] None of the above
- [ ] Other
- [ ] I don't know

* Who should have the weight in bearing the responsibility for setting up cybersecurity safeguards for protection against cyberattacks?

- ( ) Industry actors (manufacturers, connectivity providers, telecom providers, digital service providers, etc.)
- ( ) Public actors (e.g. Member States' governments, EU authorities)
- (●) Both
- ( ) I don't know

* In order to get a full overview of security gaps leading to cyberattacks, also other actors of the mobility ecosystem, currently not covered by the Directive on the security of network and information systems (NIS), but that could be affected by cyberattacks on critical infrastructure and that could cause a spill-over

effect on the mobility ecosystem, should be invited to take part in the cooperation mechanisms to discuss cyber matters established under the NIS Directive (e.g. car manufacturers of self-driving cars, cloud service providers processing the data of the self-driving car, etc.).

- ○ I strongly disagree
- ○ I disagree
- ○ I agree
- ◉ I strongly agreee
- ○ I don't know/Not applicable in my case

If you have any comments on this section, please, insert your comment here:

800 character(s) maximum

Data governance and data protection issues

Connected and automated vehicles will generate a large amount of data that could be shared through communication devices. These data have an enormous potential to create new and personalised services and products, revolutionise existing business models (e.g. roadside assistance, vehicle insurance, vehicle repair, car rental, etc.) or lead to the development of new ones. Different economic actors are competing for such data.

The issue of access/exchange/reuse of in-vehicle data is still emerging and to date there is still no data governance model that is widely accepted across stakeholders. Current data protection rules in place ensure the conditions under which some of these data (e.g. personal data) can be shared. The real benefits of connected mobility for the citizens would develop if access to these data is given to also other car digital service providers than the car manufacturers. For the time being, there is no legal obligation to ensure access to this data among the various actors of the mobility ecosystem once the data subject has authorized the collection of its in-vehicle data. In practice, the car manufacturers are the ones who organise de facto this access. Therefore the Connected and Automated Mobility (CAM) Communication proposed to monitor the current situation, as well as to consider options that will ensure the implementation of the general principles proposed in it (i.e. fair competition, end-user's freedom of choice, safety, cybersecurity, and personal data protection, covered by the e.g. General Data Protection Regulation, ePrivacy Directive).

The aim of this section is to identify a set of actions that the Commission could recommend in the meantime to member States to implement the set of principles laid out in the CAM communication for testing and pre-deployment to foster data access, sharing, processing and storing, highlighted as relevant by the industry stakeholders, end-users and national authorities.

Until the data is anonymised, typically all vehicle data collected will be considered as personal data under the General Data Protection Regulation (GDPR). While the Recommendation must be in full compliance with the rules set by the GDPR, specifically the lawfulness of processing of data (art. 6), the conditions for consent (art. 7) and the portability of data (art. 20), the collection and processing of personal data imply that car digital service providers have access to personal information. Based on the processing of their personal data, the individuals concerned may be subject to practices such as, for example, differentiated pricing, targeted advertising or refusal of services. There are also privacy risks associated with the potential of cyberattacks committed on these data.The ePrivacy Directive – and once adopted, the ePrivacy Regulation – may also be relevant in some situations to help protect the confidentiality of personal communications.

* Do you see business potential for the re-use of non-personal in-vehicle data (e.g. anonymised data)?

- (●) Yes
- ( ) No
- ( ) I don't know

* If you replied "Yes" above, please explain your choice.

800 character(s) maximum

EPIC supports and recognizes the importance of using anonymized data for research, the development of safer vehicle features, and other necessary purposes.

* What kind of data sets do you collect most frequently when developing car digital services?

- ( ) Data concerning driving habits
- ( ) Data concerning the functioning of the vehicle
- ( ) Location data
- ( ) Data concerning the state of the roads
- (●) Other sets of data

* If you replied "Other sets of data" above, please list them.

800 character(s) maximum

Not applicable

* How do you proceed with the processing of the in-vehicle data that you collect when developing car digital services?

- (●) I anonymised all the data I collect
- ( ) I delete all the data as I do not offer car digital services
- ( ) I process the data in accordance with data protection rules
- ( ) Parts of the data sets I anonymised, other sets I process in accordance with data protection and privacy rules

* According to Art. 20 GDPR (“Right to portability”), the data subject has the right to receive the personal data he/she has provided the data controller with and has the right to transmit those data to another controller without hindrance from previous data controller. Do you have experience with the implementation of this right (e.g. have you received any data subject requests for this right, how many) ?

- (●) Yes
- ( ) No, I have not received any request of this kind

* If you replied "Yes" above, please describe how you implemented this request in practice.

800 character(s) maximum

Not applicable

* Specific guidance on how to implement existing data protection rules (e.g. General Data Protection Regulation, ePrivacy Directive) in the context of connected and automated mobility would be helpful.

- ( ) I strongly disagree

- ○ I disagree
- ○ I agree
- ◉ I strongly agree
- ○ I don't know/Not applicable in my case

* Would access to in-vehicle data help you, as industry actor, develop more data services/products when connected and automated vehicles are fully deployed?

- ○ Yes
- ○ No
- ◉ I don't know

* GDPR establishes rules for processing of personal data, also the sharing of that data (e.g. giving access to it). Under Article 6 GDPR , a legal basis is needed to collect and to share personal data (for instance, consent of the individual concerned, a contract or a law). There is a need to provide for access to in-vehicle data by operators other than car manufacturers:

- ○ I strongly disagree
- ○ I disagree
- ○ I agree
- ○ I strongly agree
- ◉ I don't know/Not applicable in my case

* Which of the below processes should be prioritised in relation to providing for the access to in-vehicle data once the data subject has given the authorization for the collection and the sharing of the data?

- ○ Industry-led approaches (contractual arrangements, voluntary standardisation)
- ◉ Regulatory measures (including EU level measures imposing a legal obligation to share in-vehicle data once the data subject has given the authorization for the collection and the sharing of the data)
- ○ EU guidance to Member States on access and re-use of in-vehicle data for testing in addition to the general principles laid down in the Connected and automated Communication.
- ○ Standardisation on access and exchange of in-vehicle/road transport data
- ○ All of the above
- ○ None of the above
- ○ Other
- ○ I don't know

* If needed, who should determine the rules to be put in place on how access to in-vehicle non-personal data should be handled and protected? (You can pick more than one answer)

- ☐ Automotive suppliers (Tier 1, Tier 2, …)
- ☐ Automotive downstream market
- ☐ Telecom providers
- ☐ Original Equipment Manufacturers
- ☐ Vendors
- ☑ Standardisation body
- ☑ Public authorities (road authorities, municipalities, etc.)
- ☑ The EU

* The Connected and Automated Mobility (CAM) Communication makes reference to some principles for the access to vehicle data and resources: fair competition, consumer choice, safety, cybersecurity and personal data protection. Do you see current/emerging solutions that would meet the requirements of these principles?
Please explain what solution/s, why this solution/s and which would be the necessary steps (technical, regulatory, etc.) for implementation.

800 character(s) maximum

Privacy by design—all developers and manufacturers should “bake in” secure technology to protect against security breach; Data minimization—all parties involved in the mobility ecosystem should minimize the scope of data collected and only collect what is absolutely necessary to effectuate a legitimate purpose; Transparency—Mandatory point-of-sale labels/disclosures should be available to the consumer that explain the extent of data collection and what control the consumer has over data collection practices; Increased consumer control—Consumers should be given the choice to consent to certain data collection practices and refuse consent for others, without impacting usability of the vehicle.

* Which principles should be further developed? (You can pick more than one answer)

- [ ] Fair competition
- [ ] The possibility for consumer to have access to different services
- [x] Safety
- [x] Cybersecurity

* In relation to the previous question, please explain your choice.

800 character(s) maximum

Principles protecting consumer safety and cybersecurity should be prioritized over industry interests.

* What would be your preferred technical solution for accessing in-vehicle data and resources in a short /medium term? Please explain why and what would be the necessary steps (technical, regulatory, etc).

800 character(s) maximum

All data collected and used must be completely de-identified. Navionic systems should be kept separate from Internet-connected entertainment features. For more information, see, https://epic.org/amicus/cahen/

* Should the access/reuse of (some) in-vehicle data only be allowed to some industry actors? Please explain your answer.

Not applicable

* When re-using in-vehicle data or when willing to access in-vehicle data have you encountered any restrictions or disadvantageous situations in comparison with other service providers?

- ( ) Yes
- ( ) No
- (•) Other

* If you replied "Other" above, please specify any other reason in which you have been prevented to re-use in-vehicle data for commercial or non-commercial purposes.

800 character(s) maximum

Not applicable

* The European Commission has published guidance on private sector data sharing in B2B contexts in April 2018. Do you think these principles (transparency; shared value creation; respect for each other's commercial interests; undistorted competition; minimised data lock-in) should be refined to reflect the particular nature of in-vehicle data?

- ○ No, they are already applicable in the automotive sector
- ◉ Yes, they should be adapted to include personal in-vehicle data
- ○ I don't know
- ○ Other

* If you replied "Yes" above, please specify how you would adapt these principles to reflect the particular nature of in-vehicle data.

800 character(s) maximum

It is necessary to revise the guidance to specifically incorporate the nature of in-vehicle data because of the unique types of data that the vehicle can collect (e.g. driving habits, location of detours, audio/visual recordings of the driver and passengers). Transparency, for example, should be revised to clarify these specific types of data that can be collected. Minimised data lock-in could also be revised to provide for mandatory deletion of any unnecessary data that was collected.

If you have any comments on this section, please, insert your comment here:

800 character(s) maximum

Technology

It is expected that connectivity will be a major enabler for automated vehicles. Therefore, the Commission will follow an integrated approach between automation and connectivity in vehicles. When vehicles become increasingly connected and automated, they will be able to coordinate their manoeuvres, using active infrastructure support and enabling truly smart traffic management for the smoothest and safest traffic flows.

The aim of this questionnaire is to identify if Member States need guidance in relation to the spectrum band that could be used for large scale testing and experimentation, or early deployment.

* Are you already developing or planning to develop equipment that would require specific radio spectrum?

- ○ Yes
- ○ No
- ◉ I don't know/Not applicable in my case

If you have any comments on this section, please, insert your comment here:

800 character(s) maximum

Contact

Ana-Maria.FIMIN@ec.europa.eu