



The Consumer Voice in Europe

PROTECTING EUROPEAN CONSUMERS WITH CONNECTED AND AUTOMATED CARS

Position paper



Contact: Dimitri Vergne – sustainability@beuc.eu

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2017-138 - 28/11/2017

Why it matters to consumers

Passenger cars are rapidly becoming more interconnected both within the vehicle themselves and with the wider world. Technological changes, which to a large extent have been driven by advances in communications tools and use of the internet, have presented motorists with an influx of new digital services and driving features. The potential benefits for motorists are wide ranging. However, the opportunities also present significant risks with issues such as liability, safety, data protection and fair competition within the automotive sector. These developments need to be fully addressed in order to ensure that EU consumers can benefit from greater connectivity whilst simultaneously being protected.

Contents

Introduction	2
Context and background.....	3
1. Product Liability and motor insurance	4
2. Safety	6
3. Privacy, security and data control	7
4. After-market services.....	8
5. Interoperability and cross border challenges	9
6. Obstacles to further connectivity and automation	10
7. Ethical challenges.....	11

Introduction

This paper outlines BEUC's position on connected and automated driving with a specific focus on the EU level and the measures needed to protect consumers in this area. It is important to recognise that terms such as 'connected cars' and 'automated cars' are widely used to describe many different and recent technological changes with the design and use of the passenger car. The terms in essence encompass two specific developments; being the advances in telecommunications and ongoing developments with regard to the automation of vehicles. It is important to recognise that a vehicle that is considered as connected will not necessarily be automated, but a vehicle that is semi or fully automated will almost certainly be connected. For the purpose of this paper we provide two general definitions on what the terms apply to:

- **Connected car:** A vehicle that has devices which allow for communications¹ with other devices both within and/or outside of the vehicle itself, including other vehicles, infrastructure and the wider internet.
- **Automated car:** A vehicle that allows for some driving functions (semi-automated) or all driving functions (fully automated) to be controlled without human supervision or input.

¹ By means of any electronic communication networks, covering signals conveyed by wire, radio, optical or other electromagnetic means (EU, [Accessed July 2017](#)).

Context and background

The level of connectivity and automation in vehicles available in Europe is growing and it is estimated on a global basis that a significant rise in sales of connected vehicle features will occur over the coming years (See Figures 1). The sorts of products and services associated with connected and automated (C&A) cars are growing and already numerous: From mobility management systems (i.e traffic flow information services that are provided by way of GPS) through to automated driving tools (i.e keep your lane systems/cruise control/complete self-driving options) - the options are almost endless².



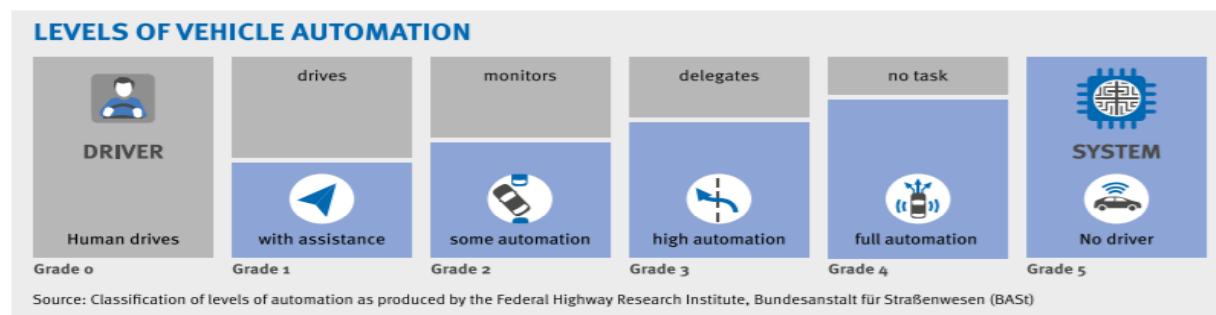
These new services and driving features offer [1 - Source: EC \(2015\)](#) numerous possible benefits to the consumer. For instance, motorists informed about the location of available parking spaces might mean less time spent driving, less urban congestion, lower fuel costs and emissions and could help reduce driver stress. Semi and fully automated vehicles (depending on the level of automation – See Figure 2) offer new driving experiences, more free time to drivers, and the latter option could potentially mean that a vehicle is completely free of driver involvement, in turn opening up new possibilities for consumers who otherwise would not drive.

However, such services and driving features that have and will continue to be brought to the market as a consequence of greater connectivity also throw up a number of risks that require measures to be taken in order to protect consumers and wider society. **Surveys show that consumers are concerned about the consequences of greater vehicle connectivity and automation.** For instance, BEUC's German member Verbraucherzentrale Bundesverband (vzbv) [conducted a survey](#) in 2016 that showed over 60% of respondents were concerned about data protection and liability with connected cars and 80% were worried about cyber security and the possibility of vehicle hacking with automated cars.

There are indeed numerous and often interlocked challenges that need to be tackled with regard to the further deployment of C&A vehicles, including: issues surrounding liability, safety, data protection and security, insurance, fair competition and interoperability to name a few. This paper outlines BEUC's position on the key issues where action is needed urgently so as to ensure that consumers are better protected and can benefit from the deployment of more connected and automated vehicles.

These challenges are exacerbated by the **availability of different ownership, car-sharing and ride-sharing models**. Consumers today can own, lease or rent a car, but they can also pay to have access to shared mobility services such as car clubs, mobility as a service models such as Car2Go or DriveNow, or ride-hailing services such as Uber or Blablacar. It is important to analyse the issues highlighted above in light of these different mobility models as they will have different implications in terms of liability, access to data, insurance, competition, etc.

² See detailed list by [PWC \(2014\)](#).



2 - Source: VZBV (2016)

1. Product Liability and motor insurance

Product liability

Product liability law is a legislative response to the risks that arise from defective products. The principle of liability without fault - for situations where defective products cause harm or damage - fulfils a compensatory function. It follows the rationale that the one who makes a profit from dangerous activities should be held accountable if this danger materialises - for instance in the form of a motor accident.

The European Commission is currently reviewing existing EU product liability legislation, which has not been significantly updated since its inception in 1985. There is a need to reform the legislation so that it adequately covers advances with all connected and automated products, including C&A vehicles. In its current format, the Directive fails to capture several relevant issues (See Box 1 for an overview of some of the key points in [BEUC's dedicated position paper on product liability](#)) and for this reason the Directive needs to be reformed in order to build consumer confidence in C&A vehicles for the current day as much as for the future.

Box1. EU liability rules are not in sync for C&A cars, among them:

Digital services: The Directive applies to movable products only, excluding services. It is therefore unclear whether it would apply to digital technologies, such as embedded software, cloud services, or indeed the in-car systems of C&A vehicles.

Definition of a defect: A product is 'defective' when it does not provide the 'safety which a person is entitled to expect'. Yet, this safety concept is imprecise, particularly when it is considered in regard to digital goods which may require software updates, including those in C&A cars.

Exceptions to liability: It is unclear how the exceptions for liability apply to digital products. There is a concern here under the scenario where a defect manifests itself after the product has gone on sale – something that is particularly concerning with cars being their long life expectancy and obvious safety risks.

Definition of liable persons: The Directive's definition is inappropriate when it comes to the Internet of Things - there is a problem e.g. with identifying the liable person when the same product is made by several manufacturers – with C&A cars there are multiple parties involved in vehicle production.

Burden of proof: Under the current system, there is too much burden on the injured party to prove a defect. It should be sufficient for the injured party to prove that a damage resulted from the product, whilst it should be for the producer to prove that the car was safe. At the very least, the existence of a damage resulting from a product should be considered as *prima facie* proof that the product is defective. With cars today, such solutions would strike a better balance of liability as (only) car makers have full access to safety records.

Data recorders (black boxes) inside vehicles have also been proposed to help identify accident liability. It is essential that any use of data recorders fully respects the principles of the General Data Protection Regulation (GDPR, see section 5) and that clear rules are in place concerning their use, access and transparency. Ultimately, if a car maker can fit a defeat device³ to an emissions control system, it should come as no surprise that a car maker might deliberately try to manipulate event data recorders to avoid incriminating evidence. Robust regulations are essential.

Motor insurance

With regard to motor insurance, there are concerns about how personal driving behaviour data is managed and controlled (See [Derikx et al, 2015; Consumentenbond, 2016](#)). The fear is that motorists could lose control of their personal data and in turn be unfairly penalised by an insurance provider. There is a question about what sort of information would be legitimate for an insurance provider to consider when setting premiums (e.g. if a motorist often drives to an economically disadvantaged area and this can be captured in the driving data, would this be valid information for an insurer to consider?). Another concern here relates to the consequences for those consumers who want the right to be 'unconnected' or whom choose not to share their data. They might also face being discriminated against.

A formal review of the motor insurance Directive is expected in 2017. This should be an opportunity to ensure the Directive is fit for purpose and adequately protects consumers with regard C&A vehicles. There is good reason on a macro level at least why the current legislation needs a review: Not only does the legislation not differentiate between a vehicle that is controlled by a human compared to one that is 'automated', it only refers to insurance policy holders as 'persons'. The sector is clearly evolving rapidly with some car makers indicating advanced levels of automation (levels 3-4) to be available in the early 2020s. Rather than waiting until further automated cars are brought to market, it would be advisable to future proof legislation, and in turn avoid treating consumers like guinea pigs for medical trials.

BEUC proposal:

- The Product Liability Directive needs a comprehensive reform in order to fully account for the technological developments concerning all connected and automated products, including passenger cars.
- The use of black boxes must be strictly regulated in accordance with the EU data protection regulations and ensure the highest levels of privacy and transparency in their use.
- BEUC calls for a full review of the EU Motor Insurance Directive to ensure it is fit for purpose for connected and automated vehicles.

³ A defeat device is a [motor vehicle](#) software or hardware that interferes with [emission controls](#) under real world driving conditions. As a consequence a vehicle may pass formal emission testing in a laboratory but emit much higher emissions when being used on the road.

2. Safety

Type approval and market surveillance

Consumers must be assured that the products they are using are safe and reliable. To ensure this is the case with C&A cars, vehicles must be robustly tested. Most EU vehicle safety regulations are developed at the UN level ([UNECE, 2012](#)). It is expected that further UN legislative changes will be made in the coming years due to technological advances which will directly impact on EU regulations, most notably EU type approval legislation. It is essential that the UN and the EU strive for the most rigorous checks on C&A vehicles before they go on sale, and suitable market surveillance activities once on the road. Such checks should include rigorous 'penetration testing' – where by a deliberate attempt to break into the security safeguards of a vehicle is conducted – and checks on software updates to ensure the car is still in compliance with type approval. Manufacturers should provide access to algorithm and software used for decision-making in C/A vehicles to independent organizations. External observers should be able to conduct third party checks.

Consumer information

In regard to semi-automated driving features, there are concerns that companies are providing consumers with misleading information about their capabilities. For instance, in 2016 the German Minister for Transport [called on the US car maker Tesla](#) to refrain from using the term 'Auto Pilot' on the basis that it was misleading consumers. Several other car makers are offering semi-automated systems in their vehicles and these developments are set to grow in the coming years. It is clear that car makers should be providing clear information to consumers that does not give a misleading impression about the capabilities of C&A vehicles and that such information is provided both at the point of purchase but also during the life of the vehicle. In-vehicle display systems should provide reliable information about the level of automation of the vehicle and the related rights and duties of the driver. The EU should make a full assessment of information being presented to consumers with regard automated systems and in turn review the need for adopting some minimum EU requirements for labelling purposes.

Driver Training

The primary goal of C/A vehicles is to facilitate driving and improve the customer experience. However, they also pose new challenges for motorists and will certainly require specific driving skills. The European Driving License Directive should lay down minimum requirements for learner drivers, and those renewing licences, to better understand the user requirements of C&A driving features.

BEUC proposal:

- Ensure that type approval and market surveillance regulations are fit for purpose for testing connected and automated cars.
- Car makers should ensure that consumers are provided with clear information about automated tools before sale and throughout the use of the car.
- The EU should assess the consumer information provided by car makers about automated vehicle systems and if necessary propose minimum labelling requirements.
- EU Driving license rules must be updated so that learner drivers, and those renewing licenses, have the expertise to handle new connected & automated technologies.

3. Privacy, security and data control

Data protection

The EU's General Data Protection Regulation (GDPR) lays out the legal framework for the protection of personal data. It represents a significant step forward but also has some weaknesses. One of the weaknesses in the Regulation is the vague definition of what is considered a "legitimate interest" to process data without consumer consent. There is a concern that industry might misuse such a concept. What is also unclear about the legislation is how it should be applied with regard C&A vehicles and therefore guidance should be produced to aid the implementation of the legislation.

Privacy in the digital world

Strong legislation to protect consumer's privacy in the digital world is also necessary. In 2017, the Commission made a proposal to reform EU legislation on privacy and electronic communications (e-Privacy Regulation). The legislation would apply to all connected products including C&A vehicles. Here, there are several areas where the Commission's proposal should be strengthened. For instance, it is essential that 'Privacy by default' obligations are included, that software default settings are configured to guarantee the highest level of privacy from the outset; and it must ensure that the tracking of the physical location and movements of consumers is not allowed without asking for their consent. (See [BEUC's dedicated e-privacy position paper](#) for a full list of recommendations).

Cybersecurity

There are also additional requirements needed in order to prevent against hacking and cyberattacks. This will require common EU rules to ensure that such risks can be reduced and that wherever a motorist takes their car, they will have the confidence that security measures are equally high across Europe. An overarching consideration here should be to assess legislating on isolating critical software systems from the rest of a vehicle's internal network (alongside the need for 'penetration testing' as mentioned in Section 2). The idea of using an off-board server to isolate these software would also bear risks. All options should therefore be carefully assessed. With a specific regard to in-car payment systems, it is also essential that motorists are assured of the highest level of payment security and privacy. Here, the implementation of the Payment Services Directive must ensure this is the case.

Data control

The issue of access to vehicle data leads to the fundamental question of data control: who controls the data generated by a connected car? Most of the data generated would indeed be personal data of the driver/owner of the car and thus covered by the GDPR, but there might also be non-personal data that is generated. What rights does the consumer have over the non-personal data generated by his/her connected car? Also, further complexities arise in situations where the driver might not be the owner of the car, or, eventually when we think about future scenarios involving self-driving cars which have no driver and no owner. Legal certainty is needed to address the data control issues and ensure that ultimately it is the consumer who is in the driver seat when it comes to the usage of the data generated by his/her connected car.

BEUC proposal:

- BEUC supports the European Commission's proposal to reform e-privacy rules and must ensure that a robust legal framework is established that protects consumers' fundamental rights to privacy and data protection with their cars.
- Specific guidance is needed on how the principles of the General Data Protection Regulation (GDPR) should be implemented with regard to connected and automated vehicles.
- The EU should develop common security standards for all communications concerning connected and automated vehicles.
- The implementation of the Payment Services Directive must ensure the highest level of payment security and privacy for in-car purchases.
- Questions related to 'data control' should be thoroughly analysed. It must be ensured that, ultimately, it is consumers who are in control over the personal and non-personal data generated by their connected cars.

4. After-market services

As far as the after-market service sector is concerned, there are concerns about the level of competition that will exist as a result of attempts to gain access to vehicle data. Here, there are concerns that business sectors, such as independent repair and maintenance providers (who are likely to become more dependent on vehicle data) will be squeezed out of the market by those who have produced the vehicles, components and software. This could in turn reduce competition, reduce consumer choice and ultimately lead to increased service costs.

The issue of accessing vehicle data is strongly related to EU legislation in the areas of data protection and e-privacy (See section 3) but there is also a debate about having a vehicle specific mechanism to controlling access to vehicle data. It is vital here that any approach to managing the access, storage and sharing of vehicle generated data must be fair to all service providers while ensuring full respect of data protection law and the principles of privacy by design and by default. Furthermore, consumers should have the possibility to revoke any prior consent given to a specific data processing, and to object to the processing of their data. This has to be made possible without any technical or organizational constraint and the tools provided to register this refusal should be accessible, visible and efficient. The General Data Protection Regulation (GDPR) also introduces a new right to data portability. It is essential that consumers can easily port their car data from one service to another, to enable them to benefit from all the advantages that connected technology can bring and avoid 'lock-in' effects. Car manufacturers and service providers need to make sure that the technical measures necessary to enable data portability are developed and put in place.

BEUC proposal:

- Car makers and service providers should guarantee fair access, storage and sharing of vehicle data while fully respecting data protection laws and the principles of privacy by design and by default.

5. Interoperability and cross border challenges

There are also challenges for C&A cars when considering their use, and that of their in-car driving features, both at a national and European level.

Geoblocking

Consumers are often prevented from using, and purchasing products online, in another Member State. This is because some companies erect artificial barriers in what is supposed to be a borderless Single Market. In the EU, consumers should be able to purchase products and services from the retailer or supplier of their choice, and use them where ever they are in the EU. With connected cars, and the use of infotainment systems by passengers for instance, it is essential that consumers can benefit from being able to utilise such systems without being penalised in this respect. The upcoming Geo-blocking Regulation is a unique opportunity to tackle (part of) this problem (see [BEUC's dedicated position on geoblocking](#)).

Interoperability of electric cars

Today, owners of electric cars (that inevitably are heavily reliant on connectivity) are often faced with the challenge of having the correct payment, RFID card or online app that are supported by a specific charging point – at both the local and European level. The EU Alternative Fuels Infrastructure Directive requires Member States to ensure that public charging points are ‘accessible on an open and non-discriminatory basis to all users’. It is essential that a thorough review and necessary corrective actions are taken to ensure that the authentication and payment systems for charging stations are not penalising or causing undue inconvenience to consumers.

BEUC proposal:

- The upcoming Geo-blocking Regulation is a unique opportunity to (in part) ensure that consumers are not blocked from buying or using goods, services or digital content in their cars.
- The implementation of the Alternative Fuels Infrastructure Directive must be reviewed to ensure that public charging stations for connected and electric cars are open and non-discriminatory for consumers.

6. Obstacles to further connectivity and automation

Increasing the level of vehicle connectivity and automation throws up a number of obstacles that need to be overcome. To function and deliver their full potential benefits, it appears that C&A cars will require extensive communication (e.g. telematics, and wireless technologies) and secure, stable, and widespread high-speed mobile broadband connectivity (e.g. 5G). For consumers it will be essential that a competitive market exists and whereby easy switching is possible between connectivity providers. There are also questions here over the costs associated with these developments, the standardisation requirements and whether there are health risks associated with the use of such technologies (European Parliament, 2016). It is essential that at the European and national level a robust consumer-focused impact assessment is made of the costs and benefits of further connectivity. Furthermore there needs to be adequate investment in roaming infrastructure to ensure the safety of vehicles operating cross borders within the EU.

BEUC proposal:

- The EU should collectively and rigorously assess the extensive technological developments that are necessary for further levels of connectivity and automation, including the cost impacts, standardisations requirements and possible safety/health risks.

7. Ethical challenges

Finally, the deployment of semi and fully autonomous cars poses difficult ethical dilemmas. There are ultimately decisions that will have to be taken by policy makers, industry and consumers with regard the level of trust that can be given to these new technologies. There are some overarching questions specific to automated cars concerning safety and the decision making process of a car when confronted with a possible accident. There are also clearly unanswered aspects that have been highlighted in the different sections of this paper (i.e. the processing of driving behaviour information/liability question marks etc.). It is clear that many of these ethical dilemmas demand the input from a holistic array of experts. BEUC recommends that the European Commission launches a multi stakeholder Forum to investigate the ethical aspects of automated driving and its impact on society. This could in turn lead to European guidelines (or a Code of Conduct) for the manufacturers of automated technologies, as proposed by the European Parliament (EP, [2017](#)) and in a similar vein already developed at a national level in Germany (BMVI, [2017](#)).

BEUC proposal:

- The European Commission should launch a forum to assess the ethical principles of automated cars and in turn develop EU guidelines to better protect the interests of consumers in this rapidly developing market.



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.