European Journal of Futures Research

RESEARCH ARTICLE Open Access

Will vehicle data be shared to address the how, where, and who of traffic accidents?

J. C. F. de Winter[1,2], D. Dodou[1*], R. Happee[2] and Y. B. Eisma[3]

Abstract

Vehicles are increasingly equipped with sensors that measure the state of the vehicle and surrounding road users. Although most of these sensor data currently remain local to the vehicle, the data could be shared with the aim to improve road safety. We postulate that there is a range of scenarios regarding data sharing, with two extremes: In scenario 1, the acquired shared data will be analysed regarding the how, where, and who of road traffic errors, violations, and accidents; actions can then be taken to improve automated driving systems, manage accident hotspots, and provide personalised feedback, rewards, or penalties to road users. In scenario 2, the recorded data will not be shared, because of privacy concerns. We conclude that there exists a tension between a position of utilitarian use of data and a position of privacy.

Keywords: Automated vehicles, Traffic violations, Traffic accidents, Driver behaviour, Profiling

Introduction

Road traffic accidents are a serious public health problem. The lifetime odds of dying in a motor vehicle accident in the USA has been estimated at 1 in 114, which is high compared to, for example, air transport accidents (1 in 9821) [1]. Young people are overrepresented [2], making road traffic accidents a large societal problem in terms of disability-adjusted life years (DALYs). Compared to technical failures, human failures are a much larger contributor to accidents [3]; human errors (e.g., inattention, loss of control) and violations (e.g., excessive speed) both contribute to accidents [4–7].

Automotive manufacturers devote large amounts of resources to further develop advanced driver assistance systems (ADAS), such as adaptive cruise control (ACC), automated emergency braking (AEB), lane keeping assistance (LKA), electronic stability control (ESC), and intelligent speed adaptation (ISA). Partially automated driving systems, where drivers can remove their hands from the steering wheel for periods of time, are now also being deployed. In addition, ICT companies, such as Waymo (currently worth 175 billion USD [8]), are continuously improving the software of their automated vehicles. According to data from May 2017, 30 manufacturers have permission from the California Department of Motor Vehicles to test automated vehicles on Californian roads [9]. Despite these rapid developments, it has been argued that it may take at least six decades before fully automated cars can drive safely on all public roads with the driver entirely removed from the control loop [10]. As the uptake of automated vehicles will happen gradually, automated vehicles will share the roads with human road users such as manually driven cars, cyclists, and pedestrians. Thus, future traffic will be mixed.

The sensors of ADAS and automated vehicles sense not only the state of the host vehicle but also that of road users in the vicinity. Ohn-Bar and Trivedi [11] provided an overview of ongoing research activities in three areas where sensors measure human behaviour: (1) measuring the human in the vehicle (e.g., distracted/attentive, hands on wheel), (2) measuring humans around the vehicle (e.g., cyclists'/pedestrians' intent, trajectory, attention), and (3) measuring humans in surrounding vehicles (e.g., whether the driver in a nearby vehicle is attentive). Automated vehicles will be able to not only classify all road users in a traffic situation ([12–15]; Fig. 1a) but also make short-term predictions of the behaviours of those road users ([16]; Fig. 1b), allowing the automated vehicles to drive in dense city environments.

* Correspondence: d.dodou@tudelft.nl
[1]Department of BioMechanical Engineering, Faculty of Mechanical, Maritime and Materials Engineering, Delft University of Technology, Mekelweg 2, 2628 CD Delft, the Netherlands
Full list of author information is available at the end of the article

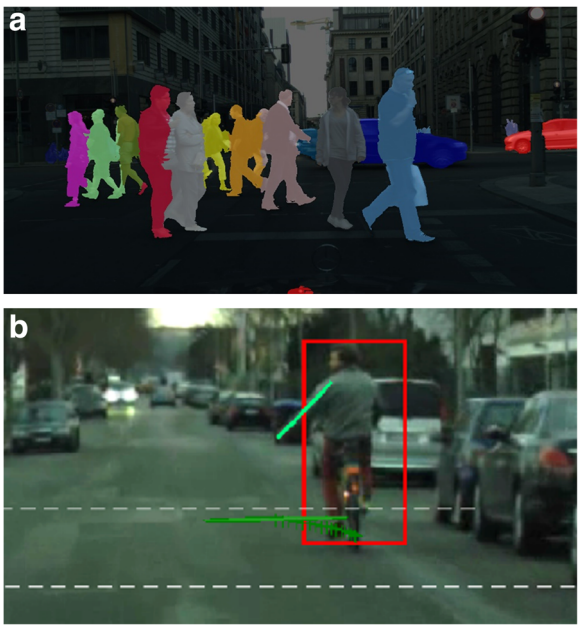

Fig. 1 In the future, it may be possible to not only **a** classify all individual road users in the environment (pixelwise instance segmentation [79] of an image from the Cityscapes Dataset [80]) but also to **b** predict their paths. The snapshot shows the predicted path (green curve) and position (green patch) of a cyclist (red box) 1 s into the future. Here, the cyclist is about to initiate a left turn at an intersection (horizontal dotted lines). From Kooij et al. [16]

In this paper, we argue that the data that are recorded by automated vehicles have *additional* potential to contribute to reducing the number of traffic accidents. In order for their potential to be unlocked, these data will need to be shared beyond the vehicle itself so that they can be used to analyse the how, where, and who of road traffic errors, violations, and accidents.

We postulate that there is a range of scenarios of data use, with two extremes: in scenario 1, the collected data will be widely shared and used, whereas in scenario 2, the collected data will not be shared. That is, in scenario 2, society will not analyse, make decisions, or implement actions based on the data that are collected by vehicle sensors. Below, we describe these two extreme scenarios. Although the level of future data use will likely lie between these two scenarios, describing these two extremes aids identifying the potentials and bottlenecks of data use.

Scenario 1: The collected data of road users' behaviours will be used at their full potential

How do errors and violations lead to accidents?

Consider a situation where a motorcycle encounters an automated vehicle. The rider does not pay attention and crosses the road without having priority. Although the vehicle performs an emergency braking manoeuvre, the vehicle and the rider collide, and the rider is fatally injured.

The vehicle sensors have recorded the sequence of behaviours and events that led to the accident: the speed and path of the automated vehicle and the rider, the braking or steering inputs of the automated vehicle, and any faults or diagnostic messages, as well as camera recordings of the accident. That is, instead of the inferential and circumstantial data that are typically used to reconstruct an accident, the vehicle sensors have collected all physical and behavioural data (including errors and violations), creating several opportunities for data use to prevent future accidents.

First, the automated vehicle could transmit the sensor data to the automotive manufacturer, and the manufacturer could use these data to improve the predictive ability of the computer vision algorithms. Such techniques are already deployed, albeit at a limited scale. For example, Tesla wirelessly transmits data (e.g., "about various driving and vehicle conditions, including braking, acceleration, trip and other related information regarding your vehicle." [17]) to Tesla service technicians, so that the data are analysed and updates are rolled out [18]. A few months after the fatal crash in May 2016, where the forward-looking camera of the car failed to see a white truck against the bright sky, Tesla deployed an update that allows for more advanced signal processing using the in-vehicle radar [18].

Second, the data could be shared with other organisations. In particular, the automotive manufacturer may (have to) share the data with a transportation safety board, so that the accident is investigated and the responsible parties are held accountable. After a self-driving Uber fatally hits a pedestrian in Arizona on March 18, 2018, the National Transportation Safety Board required Uber to share "any and all electronic data stored on the test vehicle or transmitted to Uber" [19] as well as a video recorded by a dash camera in the vehicle [20]. Considering the seriousness of the accident, the manufacturer could also decide to share the information with other manufacturers or even deposit (an anonymised version of) the data in a database accessible by scientific researchers. The next step is the Internet of Vehicles, a decentralised network in which the cars are sensor platforms that share data among each other and with road infrastructure in a collaborative manner [21].

The data that are recorded by an automated vehicle do not have to be shared over a wireless network to prevent future accidents; the knowledge that is available inside the automated vehicle could also be shared *directly* with other road users to prevent imminent accidents. For example, besides slowing down or performing an evasive manoeuver, the vehicle could automatically communicate a horn sound in an attempt to direct the rider's attention (Fig. 2a).

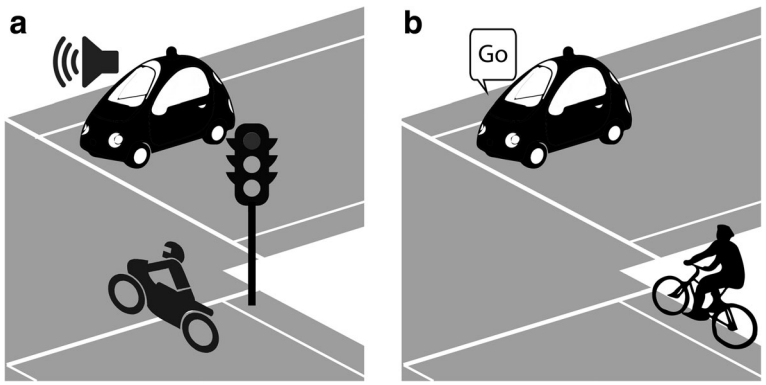

Fig. 2 Possibilities for giving real-time feedback if an automated vehicle detects **a** a hazard or **b** an inefficiency

Above, we used a fatal accident to illustrate opportunities for data sharing. Similar opportunities exist with any recorded aberrant behaviour that results in a near miss or inefficiency. Besides automatically issuing a horn sound as mentioned above (Fig. 2a), the vehicle may signal "Go" to make a traffic situation more efficient (Fig. 2b; see also [22]).

In summary, if sensor data were shared (either wirelessly to scientists and technology developers, or directly to other road users), the *how* errors and violations lead to accidents would be elucidated, the development of automated vehicles would accelerate, and road safety could benefit. The sharing might concern the aetiology of accidents, but could just as well be extended to non-hazardous-but-inefficient road users' behaviours.

Where do errors and violations occur?

The identification of accident hotspots is traditionally done based on historical accident data. Sensor data by automated vehicles can improve the identification of accident hotspots in two ways. First, in-vehicle sensors (so-called floating car data) cover a much larger portion of the road network than current road-side radar measurements [23, 24]. Second, if sensor data by automated vehicles are sent via a wireless connection and stored in a central database, researchers could use these data to pinpoint where not only accidents but also errors and violations occur. As an example, Ryder et al. [25] proposed an in-vehicle system that records near-accidents in the form of hard braking and evasive manoeuvers in order to enrich hotspot databases.

Knowing where errors and violations occur offers several possibilities for geo-specific accident prevention. First, if a particular intersection yields a high amount of errors and violations (e.g., close encounters with vulnerable road users), then the intersection could be redesigned (e.g., adding lane markings, traffic lights, or a roundabout) before an accident has occurred at that site. Kieć et al. [26], for example, combined floating car data with video observations to compare the safety of turbo-roundabouts with and without lane dividers.

Additionally, if road authorities have established which locations are prone to errors and violations, it will be possible to warn drivers in real time that they are entering a traffic location that is statistically hazardous. For example, current route navigation devices provide warning sounds regarding the presence of speed cameras and accident hotspots [27]. Similarly, the error- and violation-prone locations as identified by the analysis of floating car data could be communicated to road users, including specific information about the type of errors and violations occurring at that location (e.g., road sections where drivers drive close to other vehicles or exceed speed limits).

In summary, data sharing will enable a better understanding of *where* road accidents occur. This understanding could allow for a smart redesign of road infrastructure and personalised warnings to non-automated road users (e.g., drivers of manually driven cars). Furthermore, a redesign of road infrastructure (e.g., removal of hotspots) will accelerate the deployment of automated vehicles.

Who makes errors and violations?

The theory of "accident proneness" states that certain drivers are overinvolved in accidents because of their clumsiness or personality, a theory that has often been discredited [28–30]. The typical line of argument against accident proneness is as follows: Drivers perform a psychometric test, and their accident records are collected either retrospectively or prospectively. Usually, it is found that the correlations between test scores and accidents are small (e.g., $r < 0.10$), leading to the conclusion that the notion of accident proneness should be abandoned [31]. Recent research on accident occurrence at the individual level has shown that correlations between accident occurrence and psychometric tests are small, because accidents are rare and largely due to situational

factors: Some drivers may never be involved in an accident, whereas others may be involved in an accident due to bad luck (e.g., another driver running into them, a slight lapse of attention which is unrelated to more invariant personal characteristics). However, simulation studies and empirical data suggest that if enough accident data are collected, individual accident occurrence data are reliable, with stability correlations up to $r = 0.8$ [32, 33]. This finding indicates that some drivers are more accident-prone than others. Next to accidents, drivers' behaviour also appears to be stable. For example, in his work "Fast learners: once a speeder, always a speeder?," Groeger [34] found medium-to-high stability coefficients of driving speed (r between 0.2 and 0.8).

Transmission of data collected by automated vehicles creates several opportunities for preventing accidents before happening. In particular, it becomes possible to keep track of *who* makes errors and violations. If automated vehicles are equipped with identification features (e.g., licence plate recognition), the aberrations of other vehicles can be automatically recorded in real time. Moreover, if the identification software allows for facial recognition, it will be possible to record the behaviour of non-motorised individual road users, such as pedestrians, cyclists, and motor riders. Shanghai police uses facial recognition to identify cyclists who cycle on the wrong bike lane [35, 36], and in Shenzhen, facial recognition is used to catch jaywalkers [37] (and see O'Malley [38] for a review on the technological and societal bottlenecks of "telemetric policing" techniques).

The recording of errors and violations allows for calculating a person-specific "violations score" and "errors score." For example, a cyclists' violations score could be defined as a composite of how often he or she runs a red light and ends up in dangerous encounters with other road users. Multi-day driving simulator research has shown how to calculate errors scores (based on, e.g., recorded lane keeping inaccuracies) and violations scores per driver [39] (e.g., based on speed, headway, and red light violations [40]). Various on-road studies have shown that it is possible to create a driver risk profile using sensors in smartphones (e.g., accelerometers, GPS) and vehicle sensors (e.g., [41–44]).

The automatic identification of individual (repeat) traffic offenders offers opportunities for types of remedies other than enforcement, such as personalised feedback, remedial courses, and rehabilitation programs to road users. For example, road users may receive feedback via the Internet, which they can then use to improve their behaviours (e.g., [45]). The recorded errors and violations could be also communicated to insurance companies. For example, car drivers and motorcycle riders may receive a reduction in their insurance premiums if they have low errors and violations score. According to data from November 2017, ten insurance companies in the Netherlands already offer such policies, transmitting velocity, accelerations, and GPS position via a dongle plugged into the ODB port [46]. Experiments have indicated that pay-as-you-drive and pay-how-you-drive insurance can lead to a reduction of speeding violations (e.g., [47]).

In summary, vehicle sensors may be able to record *who* makes errors and violations, which in turn permits remedial action. Of course, in a fully automated car, the driver will not make any errors or violations (because the vehicle is in control and will abide by the traffic rules). However, until all cars drive fully automatically, the aberrant behaviours of drivers of manually driven cars, cyclists, and pedestrians will be recorded by automated vehicles in the vicinity. These data could be shared with road users themselves, but also with third parties such as insurance companies and licencing authorities.

Scenario 2: The collected data of road users will not be used

The collection of large amounts of data is realistic from a technological perspective because the introduction of sensors that detect and classify road users and predict their path, intents, and future actions is inherent to increasing levels of automated driving on the road. The question, however, is whether the data will actually be shared and subsequently used to improve road safety. One main barrier to exploiting road users' behavioural data is that of privacy, especially regarding driver profiling. In this section, we address some concerns that stakeholders may have about the different stages of data processing.

- Which data should be exchanged, between which parties, and how? There have been already heated debates between automotive manufacturers, telecom operators, and the European Commission regarding which technologies should be used for data exchange (e.g., short-range Wifi or long-range 5G networks) [48]. Another relevant question concerns the duration for which the data should be kept (cf. the "right to be forgotten" as protected by, for example, Art. 17 of the EU General Data Protection Regulation, GDPR) [49].
- Who should be the owner of the data and who should have access to these data (see also [50, 51])? According to the GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

data, an online identifier" (Art. 4(1)) [52]. Are car drivers willing to upload their data to the cloud, and do they accept that these data will be stored and used by automotive manufacturers, governments, and researchers? In other words, are drivers willing to make utilitarian decisions, if it may not be beneficial for them individually and even if it could make them liable in case they violated the rules or cost them insurance premium? Will automotive manufacturers, OEMs, and other stakeholders who wish to use personal data collected by automated vehicles need the consent of the users/customers for doing so? Fundamental differences between Europe and the USA with respect to data ownership and data privacy will further complicate data sharing [53]. Privacy issues will become especially severe when driving skill and driving style indicators are intended to be combined with other databases, such as databases of crime, tax income, or even polygenic scores [54] (and see [55] for an overview of possible behavioural biometrics).

- How to ensure that all road users are treated fairly? A fairness criterion may require standardisation and certification of measurement devices and alliances between automotive manufacturers [56]. The computed measures further need to be standardised for vehicles of different dynamics (e.g., cars, motorcycles, trucks). Standardisation may also be required for hardware interfaces (such as concerning storage devices and other I/O devices) and software interfaces (e.g., data types, functions).
- Suppose that the entire sequence of events surrounding an accident, as in the rider-vehicle example above, is stored and shared, is it then possible to preserve anonymity? Anonymisation may be hard because of the clear behavioural signatures and geo-specific information.
- How should thresholds for remedies (e.g., updating road infrastructure, suspension of a driver's licence) be set? An overly tolerant criterion might be detrimental to road safety, whereas setting a too strict criterion may harm the quality of life of those prevented from driving. Figure 3 shows the results of a simulation where the correlation between violations scores and accident involvement scores is 0.6. It can be seen that screening out the 10% poorest drivers would lead to prevention of 39% of accidents. Naturally, there are also misses (people with a low violations score who are still involved in an accident) and false positives (people with a high violations score who are not involved in an accident). It should be noted here that although the

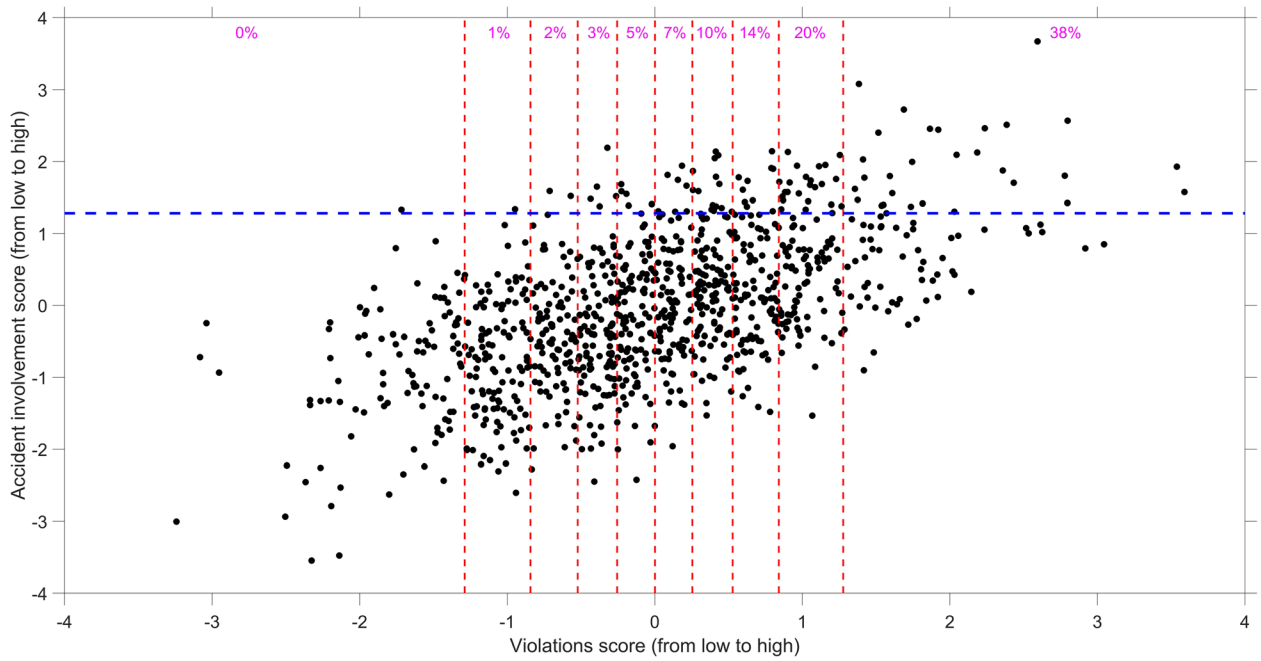

Fig. 3 Scatter plot of 1000 drivers with a correlation $r = 0.6$ between drivers' accident involvement scores and violations scores. The horizontal blue line is drawn at the 90th percentile of the accident involvement score; it is assumed that drivers with an accident involvement score higher than the 90th percentile will be involved in an accident (i.e., the overall accident rate is 10%). The vertical red lines are drawn at each 10th percentile of the violations score, and the percentage at the top shows the expected accident involvement rate of drivers within that percentile range of the violations score

threshold level may be ethically challenging, the same can be said about thresholds in contemporary driver testing and enforcement (e.g., tests of visual acuity, speed limits, demerit point system in driver licencing).

- Is it legally possible and ethically acceptable to issue fines to or revoke driver licences of drivers based on their high accident proneness (i.e., a statistical index of risk)? How does this differ from relying on overt behaviours only (i.e., speed or headway), as it is currently done, considering that in both cases an inference is made regarding whether a driver is a danger on the roads that could cause an accident in the future?
- If a person's violations and errors scores indicate that it is statistically likely that this person will be involved in a future accident, should a licencing authority suspend one's driver's licence, and should a transportation company find a replacement job for this person *merely* based on a statistical probability rather than a committed aberration? How does this proposition differ from current laws according to which a driver's licence may not be issued or renewed in case of a medical condition that is likely to impair one's driving ability or in the case of a "negligent or incompetent operator" [57]?
- As automation will become increasingly safe, information regarding unsafe manual driving could be used to enforce automated driving in specific conditions. However, the question is should all violations and other illegal acts be prevented? For example, motorised vehicles may be designed to function only within a given envelope of speed and accelerations so that some types of violations become impossible, or a vehicle can be automatically brought to a stop if the human driver exhibits dangerous behaviour (and see [58] for a discussion on whether crime in general should be made impossible or not). This question is akin to whether intelligent speed adaptation (ISA) should be enforced or not [59].

Discussion

We argued that, in the future, an increasing amount of behaviours on the roads will be recorded via in-vehicle sensors. We argued that data usage is the key to reducing the number of traffic accidents. By sharing data, it becomes possible to analyse how errors and violations relate to accidents, where these errors and violations occur, and who are more accident-prone road users than others. This information allows for remedial actions, which can contribute to reducing the number of road traffic accidents, and which may further speed up the development and deployment of automated cars.

The ideas outlined in this document concerning ubiquitous data of road users' behaviours may sound farfetched. However, it is worth noting that early versions of the required technology are already available. For example, in some countries, road-based safety cameras take photos not only of the licencing plates but also of the driver's face. Automated licence plate recognition is already commonplace, and vehicles are increasingly equipped with event data recorders and dashboard cameras. Similarly, the idea of use-based insurance (pay-how-you-drive business models) is already applied by insurance companies worldwide [60], whereas live traffic information is available from various telematics applications (e.g., [27]). Considering that Facebook's DeepFace has been used to identify people from pictures with high accuracy [61], it should also be possible to classify road users using facial recognition, provided that camera resolution is sufficient.

It is worth noting that data collected by vehicle sensors solely describe overt behaviours and not the underlying cognitive state of the road users. Human involvement will still be needed in certain types of decision-making and action implementation. For example, in a collision between an automated vehicle and a rider, the vehicle sensors measure the overt speed and path of the vehicle and the rider, but human judgement will still be needed to assess the underlying causes of the accident. Specifically, in court cases, a human judge may have to determine whether the rider was at fault and whether the rider crossed the intersection intentionally (e.g., red light violation) or unintentionally (e.g., misperception of the traffic lights).

As pointed out above, the collection of data is technologically feasible, but whether the data will actually be used is a contentious issue. Ethics of privacy are regarded as major impediments towards the widespread use of data (see [62] for public scepticism about Google Glass and [63] for privacy law considerations associated with Street View of Google Maps). It is important to note that the present discussion about the ethics of privacy differs from similar debates regarding the privacy of electronic patient files and genetic screening because the present discussion involves *public* roads. Although it is possible to keep one's medical records private, it is unlikely that road users can keep their errors and violations concealed from sensors and cameras. Moreover, while the legal status of the use of dashboard cameras differs per country [64], and current legislation in various countries does not allow event data recorders to capture audio and video data [65], the common benefit of collecting and using such data might outweigh privacy considerations in the future.

Privacy laws are stringent, but some voices argue that the "end of personal privacy" might be near in our

digitised society [66] (cf. the Internet of Vehicles discussed above). While increased connectivity creates ample opportunity for making use of the data collected by automated vehicles, these opportunities involve privacy-related ethical concerns and may, therefore, face backlash from the public. A common principle is that it is not ethically acceptable to implement and enforce systems that disclose the identity of individuals, especially when this disclosure concerns behaviours that conflict with societal and legal norms. On the other hand, this principle may have to be adapted if this could pave the way towards collective benefits such as greatly improved road safety. Here, one may wonder whether it is ethically acceptable to have over one million annual fatalities worldwide due to road accidents.

Co-standardisation of safety and security requirements, for example, by combining information security standards (e.g., ISO 15408, ISO 27001, ISO 27002, and J3061) with the automotive safety standard ISO 26262 [67], will be needed to mitigate cybersecurity risks (e.g., data tampering, hacking, fooling sensors) and convince users that their data are handled in a responsible manner. Business models that advance consumer empowerment may also play a decisive factor in users' willingness to share their data [68]: users appear to be more open in data sharing if they get benefits in return, such as financial compensation and personalised services [69–71], and when transparency and perceived justice regarding data collection, management, and processing are high [72, 73]. Secure data privacy models, transparency of data exchange, and control of third-party access are important solutions for exploiting data while at the same time complying with privacy laws [74, 75]. Fog computing, homomorphic encryption, and blockchain technology have been suggested as solutions for enabling the use of the collected data while preserving privacy [76–78].

Conclusion

By collecting large amounts of data on road users' behaviour, future automated vehicles will offer the possibility of addressing the *how*, *where*, and *who* of all aberrations and accidents on the roads. Using these data is pivotal for preventing traffic accidents, but it also generates questions about ethics of privacy. Thus, the question is not whether sensors will acquire road users' behavioural data; this is already happening and will most certainly be expanded towards more sophisticated data. Rather, the question is whether people are willing to share their data so that the data are analysed and become "information" which is then used for improving road safety. It is foreseen that in the future an increasing tension between a utilitarian use of data and a position of privacy will be dominant.

Abbreviations

ACC: Adaptive cruise control; ADAS: Advanced driver assistance systems; AEB: Automated emergency braking; DALYs: Disability-adjusted life years; ESC: Electronic stability control; ISA: Intelligent speed adaptation; LKA: Lane keeping assistance

Acknowledgements

This paper is previously published in different form as a deliverable of the Motorist project (Marie Curie ITN, Grant Agreement 608092). Joost de Winter is supported by the research programme "How should automated vehicles communicate with other road users?" (project number TTW 016.Vidi.178.047), which is financed by the Netherlands Organisation for Scientific Research (NWO).

Funding

Not applicable.

Availability of data and materials

Not applicable.

Authors' contributions

JdW conceived the study and drafted and revised the manuscript. DD co-wrote the manuscript. RH edited and reviewed the manuscript. YB assisted in writing and provided critical philosophical input. All authors read and approved the final manuscript.

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]Department of BioMechanical Engineering, Faculty of Mechanical, Maritime and Materials Engineering, Delft University of Technology, Mekelweg 2, 2628 CD Delft, the Netherlands. [2]Department of Cognitive Robotics, Faculty of Mechanical, Maritime and Materials Engineering, Delft University of Technology, Delft, the Netherlands. [3]Department of Control and Operations, Faculty of Aerospace Engineering, Delft University of Technology, Delft, the Netherlands.

Received: 12 October 2018 Accepted: 7 February 2019
Published online: 18 March 2019

References

1. National Safety Council (2017) Odds of dying. http://www.nsc.org/learn/safety-knowledge/Pages/injury-facts-odds-of-dying.aspx. Accessed 19 May 2018
2. World Health Organisation (2015) Global status report on road safety 2015. http://apps.who.int/iris/bitstream/10665/189242/1/9789241565066_eng.pdf?ua=1. Accessed 19 May 2018
3. National Highway Traffic Safety Administration (2017) Automated driving systems 2.0: a vision for safety. Introductory message from U.S. Department of Transportation Secretary, Elaine L. Chao, guidance and best practices from U.S. Department of Transportation. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf. Accessed 14 Aug 2018
4. Aarts L, Van Schagen I (2006) Driving speed and the risk of road crashes: a review. Accid Anal Prev 38:215–224. https://doi.org/10.1016/j.aap.2005.07.004
5. Klauer SG, Dingus DR, Neale TA, Sudweeks J, Ramsey DJ (2006) The impact of driver inattention on near-crash/crash risk: an analysis using the 100-car naturalistic study data. Report no. DOT HS 810 594. National Highway Traffic Safety Administration, Washington DC

6. Wierwille WW, Hanowksi RJ, Hankey JM et al (2002) Identification and evaluation of driver errors: overview and recommendations. Final report no. FHWA-RD-02-003. Federal Highway Administration, McLean
7. Treat JR, Tumbas NS, McDonald ST et al (1979) Tri-level study of the causes of traffic accidents: executive summary. Report no. DOTHS034353579TAC(5). National Highway Traffic Safety Administration, Washington DC
8. Rapier G (2018) Waymo is worth $100 billion more than previous estimates, Morgan Stanley says (GOOGL). https://markets.businessinsider.com/news/stocks/google-stock-price-waymo-worth-100-billion-more-than-before-morgan-stanley-2018-8-1027439248. Accessed 3 Oct 2018
9. Favarò FM, Nader N, Eurich SO, Tripp M, Varadaraju N (2017) Examining accident reports involving autonomous vehicles in California. PLoS One 12: e0184952. https://doi.org/10.1371/journal.pone.0184952
10. Shladover SE (2016) The truth about "self-driving" cars. Sci Amer 314:52–57. https://doi.org/10.1038/scientificamerican0616-52
11. Ohn-Bar E, Trivedi MM (2016) Looking at humans in the age of self-driving and highly automated vehicles. IEEE Trans Intell Veh 1:90–104. https://doi.org/10.1109/TIV.2016.2571067
12. NVIDIA (2017) NVIDIA and PACCAR developing self-driving trucks. https://www.youtube.com/watch?time_continue=30&v=Wweoh7WJNUw. Accessed 19 May 2018
13. TED (2015) Chris Urmson: How a driverless car sees the road. https://www.youtube.com/watch?v=tiwVMrTLUWg&t=19s. Accessed 16 Feb 2019.
14. Yu F, Xian W, Chen Y, Liu F, Liao M, Madhavan V, Darrell T (2018) BDD100K: a diverse driving video database with scalable annotation tooling. https://arxiv.org/abs/1805.04687. Accessed 3 Oct 2018
15. Greentheonly (2018). Paris streets in the eyes of Tesla Autopilot. https://www.youtube.com/watch?v=_1MHGUC_BzQ&feature=youtu.be&app=desktop#fauxfullscreen. Accessed 3 Oct 2018
16. Kooij JFP, Flohr F, Pool EAI, Gavria DM (2018) Context-based path prediction for targets with switching dynamics. Int J Comput Vis. https://doi.org/10.1007/s11263-018-1104-4
17. Tesla Motors, Inc (2012) Model S quick guide. https://www.tesla.com/sites/default/files/blog_attachments/model_s_quick_guide_-_na_rev_d_for_web.pdf. Accessed 14 Aug 2018
18. The Tesla Team (2016) Upgrading Autopilot: seeing the world in radar. https://www.tesla.com/blog/upgrading-autopilot-seeing-world-radar. Accessed 29 Sept 2018
19. National Transportation Safety Board (2018) NTSB update: Uber crash investigation. https://www.ntsb.gov/news/press-releases/Pages/NR20180320.aspx. Accessed 29 Sept 2018
20. National Transportation Safety Board (2018) Preliminary report, highway HWY18MH010. https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf. Accessed 9 June 2018
21. Gerla M, Lee EK, Pau G, Lee U (2014) Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds. In: Proc 2014 IEEE World Forum on Internet of Things (WF-IoT), pp 241–246. https://doi.org/10.1109/WF-IoT.2014.6803166
22. Nissan Motor Corporation (2015) Nissan IDS concept: Nissan's vision for the future of EVs and autonomous driving. http://nissannews.com/en-US/nissan/usa/releases/nissan-ids-concept-nissan-s-vision-for-the-future-of-evs-and-autonomous-driving. Accessed 5 June 2018
23. Aarts LT, Bijleveld FD, Stipdonk HL (2015) Usefulness of 'floating car speed data' for proactive road safety analyses: analysis of TomTom speed data and comparison with loop detector speed data of the provincial road network in the Netherlands (R-2015-3). SWOV Institute for Road Safety Research, The Hague
24. Houbraken M, Logghe S, Schreuder M, Audenaert P, Colle D, Pickavet M (2017) Automated incident detection using real-time floating car data. J Adv Trans 2017:8241545. https://doi.org/10.1155/2017/8241545
25. Ryder B, Gahr B, Dahlinger A (2016) An in-vehicle information system providing accident hotspot warnings. Prototypes 3. http://aisel.aisnet.org/ecis2016_prototypes/3. Accessed 5 June 2018
26. Kieć M, Ambros J, Bąk R, Gogolín O (in press) Evaluation of safety effect of turbo-roundabout lane dividers using floating car data and video observation. Acc Anal Prev. https://doi.org/10.1016/j.aap.2018.05.009
27. TomTom NV (2018) Live services. https://us.support.telematics.tomtom.com/app/answers/detail/a_id/3440/~/live-services. Accessed 26 Sept 2018
28. Burnham JC (2009) Accident proneness. A history of technology, psychology, and misfits of the machine age. University of Chicago Press, Chicago
29. Elvik R (2011) Book review: Anders af Wåhlberg: driver behaviour and accident research methodology. Unresolved problems. Saf Sci 49:751–752. https://doi.org/10.1016/j.ssci.2011.01.011
30. Haight FA (1964) Accident proneness, the history of an idea. Automobilismo e Automobilismo Industriale 12:534–546
31. Ranney TA (1994) Models of driving behavior: a review of their evolution. Accid Anal Prev 26:733–750. https://doi.org/10.1016/0001-4575(94)90051-5
32. De Winter JCF (2014) Why person models are important for human factors science. Theor Issues Ergon Sci 15:595–614. https://doi.org/10.1080/1463922X.2013.856494
33. Af Wåhlberg AE (2009) Driver behaviour and accident research methodology: unresolved problems. Ashgate, Surrey
34. Groeger JA (2000) Fast learners: once a speeder, always a speeder? In: Proc 10th Seminar on Behavioural Research in Road Safety, pp 144–151
35. Shanghai Municipal People's Government (2018) Traffic police target riders, pedestrians. http://www.shanghai.gov.cn/shanghai/node27118/node27818/u22ai89055.html. Accessed 5 June 2018
36. That's Shanghai (2017) Police now using facial recognition to bust cyclists in Shanghai. http://www.thatsmags.com/shanghai/post/20684/police-now-using-facial-recognition-to-bust-cyclists-in-shanghai. Accessed 14 Aug 2018
37. South China Morning Post (2018) Jaywalkers under surveillance in Shenzhen soon to be punished via text messages. https://www.scmp.com/tech/china-tech/article/2138960/jaywalkers-under-surveillance-shenzhen-soon-be-punished-text. Accessed 14 Aug 2018
38. O'Malley P (2014) Telemetric policing. In: Bruinsma G, Weisburd D (eds) Encyclopedia of criminology and criminal justice. Springer, New York, pp 5135–5145. https://doi.org/10.1007/978-1-4614-5690-2_262
39. De Winter JCF (2013) Predicting self-reported violations among novice license drivers using pre-license simulator measures. Accid Anal Prevent 52: 71–79. https://doi.org/10.1016/j.aap.2012.12.018
40. De Winter JCF, Wieringa PA, Kuipers J, Mulder JA, Mulder M (2007) Violations and errors during simulation-based driver training. Ergonomics 50:138–158. https://doi.org/10.1080/00140130601032721
41. Castignani G, Derrmann T, Frank R, Engel T (2015) Driver behavior profiling using smartphones: a low-cost platform for driver monitoring. IEEE Intell Transp Syst 7:91–102. https://doi.org/10.1109/MITS.2014.2328673
42. Johnson DA, Trivedi MM (2011) Driving style recognition using a smartphone as a sensor platform. In: Proc 2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp 1609–1615. https://doi.org/10.1109/ITSC.2011.6083078
43. Júnior JF, Carvalho E, Ferreira BV, De Souza C, Suhara Y, Pentland A, Pessin G (2017) Driver behavior profiling: an investigation with different smartphone sensors and machine learning. PLoS One 12:e0174959. https://doi.org/10.1371/journal.pone.0174959
44. Osafune T, Takahashi T, Kiyama N, Sobue T, Yamaguchi H, Higashino T (2017) Analysis of accident risks from driving behaviors. Int J Intell Transp Syst Res 15:192–202. https://doi.org/10.1007/s13177-016-0132-0
45. Dijksterhuis C, Lewis-Evans B, Jelijs B, De Waard D, Brookhuis K, Tucha O (2015) The impact of immediate or delayed feedback on driving behaviour in a simulated pay-as-you-drive system. Accid Anal Prev 75:93–104. https://doi.org/10.1016/j.aap.2014.11.017
46. Consumentenbond (2017) Korting voor je rijstijl [Discount for your driving style]. https://www.consumentenbond.nl/autoverzekering/korting-voor-je-rijstijl#no2. Accessed 4 June 2018
47. Bolderdijk JW, Knockaert J, Steg EM, Verhoef ET (2011) Effects of pay-as-you-drive vehicle insurance on young drivers' speed choice: results of a Dutch field experiment. Acc Anal Prev 43:1181–1186. https://doi.org/10.1016/j.aap.2010.12.032
48. Euractiv (2018) EU connected cars plan sparks national backlash. https://www.euractiv.com/section/digital/news/eu-connected-cars-plan-sparks-national-backlash/. Accessed 26 Sept 2018
49. The European Parliament and The Council (2016) Regulation (EU) of the European Parliament and The Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Article 17. Right to erasure ('right to be forgotten'). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504. Accessed 28 Sept 2018
50. Fagnant DJ, Kockelman K (2015) Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transp Res A Policy Pract 77:167–181. https://doi.org/10.1016/j.tra.2015.04.003

51. Kitchin R (2016) The ethics of smart cities and urban science. Philos Trans A Math Phys Eng Sci 374:20160115. https://doi.org/10.1098/rsta.2016.0115
52. The European Parliament and The Council (2016) Regulation (EU) of the European Parliament and The Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Article 4. Definitions. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504. Accessed 26 Sept 2018
53. Esteve A (2017) The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. Int Data Privacy Law 7:36–47. https://doi.org/10.1093/idpl/ipw026
54. Krapohl E, Patel H, Newhouse S et al (2018) Multi-polygenic score approach to trait prediction. Mol Psychiatry 23:1368–1374. https://doi.org/10.1038/mp.2017.163
55. Yampolskiy RV (2011) Behavioral, cognitive and virtual biometrics. In: Salah A, Gevers T (eds) Computer analysis of human behaviour. Springer, London, pp 347–385. https://doi.org/10.1007/978-0-85729-994-9_13
56. Hetzner C (2018) VW seeks industry alliance for self-driving technology. http://europe.autonews.com/article/20180914/ANE/180919890/vw-seeks-industry-alliance-for-self-driving-technology. Accessed 3 Oct 2018
57. California Legislative Information (1989) Vehicle code-VEH. §12809. http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH&sectionNum=12809. Accessed 14 Aug 2018
58. Rich ML (2013) Should we make crime impossible. Harv JL Pub Policy 36:795–848
59. Chorlton K, Conner M (2012) Can enforced behaviour change attitudes: exploring the influence of intelligent speed adaptation. Accid Anal Prev 48:49–56. https://doi.org/10.1016/j.aap.2010.06.007
60. Husnjak S, Peraković D, Forenbacher I, Mumdziev M (2015) Telematics system in usage based motor insurance. Procedia Eng 100:816–825. https://doi.org/10.1016/j.proeng.2015.01.436
61. Bohannon J (2015) Unmasked. Science 327:492–494. https://doi.org/10.1126/science.347.6221.492
62. Klein A, De Freitas AS, Pedron CD, Elaluf-Calderwood S (2015) Who is afraid of Google Glass? Mapping the controversy about wearable and ubiquitous computing. In: Academy of Management Proc, Vancouver, Canada. https://doi.org/10.5465/ambpp.2015.11235abstract
63. Strachan LA (2010) Re-mapping privacy law: how the google maps scandal requires tort law reform. Rich JL & Tech 17:1–30
64. Štitilis D, Laurinaitis M (2016) Legal regulation of the use of dashboard cameras: aspects of privacy protection. Comput Law Security Rev 32:316–326. https://doi.org/10.1016/j.clsr.2016.01.012
65. US Government Publishing Office (2011) Event data recorders–Definitions (49 CFR 571–Federal motor vehicle safety standards, Title 49, Chapter V, Part 563, Paragraph 5). https://www.gpo.gov/fdsys/pkg/CFR-2011-title49-vol6/pdf/CFR-2011-title49-vol6-sec563-5.pdf. Accessed 26 Sept 2018
66. Madan A, Waber B, Ding M, Kominers P, Pentland A (2009) Reality mining: the end of personal privacy [presentation]. https://keithlyons.me/wp-content/uploads/2011/01/ed_siii_madan_waber_et_al.pdf. Accessed 16 Feb 2019.
67. Schoitsch E, Schmittner C, Ma Z, Gruber T (2016) The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles. In: Proc Advanced Microsystems for Automotive Applications, pp 251–261. https://doi.org/10.1007/978-3-319-20855-8_20
68. Rubinstein I (2012) Big data: the end of privacy or a new beginning? Int Data Privacy Law:12–56. https://doi.org/10.2139/ssrn.2157659
69. Chellappa RK, Sin RG (2005) Personalization versus privacy: an empirical examination of the online consumer's dilemma. Inform Technol Manag 6:181–202. https://doi.org/10.1007/s10799-005-5879-y
70. Rohunen A, Markkula J, Heikkila M, Heikkila J (2014) Open traffic data for future service innovation: addressing the privacy challenges of driving data. J Theor Appl Electron Commerce Res 9:71–89
71. Liu Z, Bonazzi R, Fritscher B, Pigneur Y (2011) Privacy-friendly business models for location-based mobile services. J Theor Appl Electron Commerce Res 6:90–107. https://doi.org/10.4067/S0718-18762011000200009
72. Elia J (2009) Transparency rights, technology, and trust. Ethics Infor Technol 11:145–153. https://doi.org/10.1007/s10676-009-9192-z
73. Son JY, Kim SS (2008) Internet users' information privacy-protective responses: a taxonomy and a nomological model. MIS Quarter 32:503–529. https://doi.org/10.2307/25148854
74. Plappert C, Zelle D, Krauß C, Lange B, Mauthöfer S, Walter J et al (2017) A privacy-aware data access system for automotive applications. In: 15th ESCAR Embedded Security in Cars Conference
75. Baumann MF, Brändle C, Coenen C, Zimmer-Merkle S (in press) Taking responsibility: a responsible research and innovation (RRI) perspective on insurance issues of semi-autonomous driving. Transp Res A Policy Pract. https://doi.org/10.1016/j.tra.2018.05.004
76. Kaiser C, Steger M, Dorri A, Festl A, Stocker A, Fellmann M, Kanhere S (2018) Towards a privacy-preserving way of vehicle data sharing–a case for blockchain technology? In: Dubbert J, Müller B, Meyer G (eds) Advanced microsystems for automotive applications 2018. Lecture notes in mobility. Springer, Cham, pp 111–122. https://doi.org/10.1007/978-3-319-99762-9_10
77. Stojmenovic I, Wen S (2014) The fog computing paradigm: scenarios and security issues. In: Ganzha M, Maciaszek L, Paprzycki M (eds) 2014 Federated Conference on Computer Science and Information Systems, 2, 1–8. doi: https://doi.org/10.15439/2014F503
78. Menouar H, Guvenc I, Akkaya K, Uluagac AS, Kadri A, Tuncer A (2017) UAV-enabled intelligent transportation systems for the smart city: applications and challenges. IEEE Commun Magazine 55:22–28. https://doi.org/10.1109/MCOM.2017.1600238CM
79. Arnab A, Torr PHS (2017b) Pixelwise instance segmentation with a dynamically instantiated network. https://arxiv.org/abs/1704.02386. Accessed 19 May 2018
80. Cityscapes Dataset (2017) Detailed results. https://www.cityscapes-dataset.com/detailed-results/. Accessed 5 June 2018