Transportation Research Part F: Psychology and Behaviour 115 (2025) 103330

Contents lists available at ScienceDirect

Transportation Research Part F: Psychology and Behaviour

journal homepage: www.elsevier.com/locate/trf

Digital roads and data ethics: Exploring the road users' perspective

Rongqiu Song [a], Dimitris Potoglou [a,*], Nadeem Fayyaz [b], Mehreen Ashraf [c], Katarzyna Stawarz [b], George Theodorakopoulos [b], Tim Edwards [c], Emyr Thomas [d], Yulia Cherdantseva [b]

[a] School of Geography and Planning, Cardiff University, Cardiff, Wales, UK
[b] School of Computer Science and Informatics, Cardiff University, Wales, UK
[c] Cardiff Business School, Cardiff University, Cardiff, Wales, UK
[d] National Highways, UK

ARTICLE INFO

Keywords:
Digital roads
Road transport users
Technology adoption scenarios
Privacy concerns
Perceived benefits of digital roads

ABSTRACT

The implementation of 'Digital Roads' initiatives in the UK promises to revolutionise transportation through the integration of cutting-edge technologies such as artificial intelligence (AI) and connected vehicles. However, this technological advancement brings with it the potential for extensive data collection pertaining to road users. Understanding the concerns of these users is important for the successful adoption of these transformative transportation technologies and provides the foundation towards building user-centred ethical frameworks. This study reports evidence from five workshops with 20 participants from diverse backgrounds including computer science and cybersecurity, business, geography and planning. Each workshop captured user narratives including concerns, questions, and suggestions against three scenarios that were likely to be implemented on UK motorways in the future. The scenarios involved a hypothetical, but realistic implementation of various technologies aimed at enhancing road safety but could also be a threat to their privacy. For example, one scenario involved AI-based identification of bad driving behaviour under which participants were in turn, either a road user or the violator. The thematic analysis of the workshop data pointed towards six primary concerns: data privacy, technology reliability, data security, awareness of data collection practices, possible consequences of data collection, and the involvement of third-party entities. Addressing these concerns will be instrumental in fostering public trust and acceptance of new technologies in transportation. These findings also suggest the importance of transparency, awareness, data security, fairness, inclusivity, and accountability in ensuring data ethics within the realm of digital transportation infrastructure.

1. Introduction

Many countries have developed plans or processes to digitalise their road networks (U.S. Department of Transportation Federal Highway Administration 2020; Swedish Transport Administration 2022). For example, the United Kingdom has launched the 'Digital Roads Initiative'(National Highways 2021), which is aimed at "harnessing data, technology and connectivity to improve the way the Strategic Road Network is designed, built, operated and used" (National Highways 2024a). The 'Digital Roads' initiative envisions a

* Corresponding author.
E-mail address: potogloud@cardiff.ac.uk (D. Potoglou).

https://doi.org/10.1016/j.trf.2025.103330
Received 24 March 2025; Received in revised form 30 June 2025; Accepted 30 July 2025
Available online 6 August 2025

future in which vehicles are increasingly interconnected, and transportation systems and infrastructure evolve into smart networks (National Highways 2023).

This transformation can involve various new technologies for road transport by transforming vehicle operation, infrastructure design, and the movement of people and goods. Connected and autonomous vehicles (CAVs) can facilitate communication and exchange of information wirelessly with other vehicles, external networks and infrastructure via, for example, Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to-Everything (V2X) technologies (Liu et al. 2020). These technologies integrate sensors, wireless communications, and onboard computing systems to facilitate data exchange (Yao et al. 2023; National Highways 2024a). For example, road users can receive real-time updates about congestion and journey times, ongoing and upcoming construction, availability of parking spaces or report road incidents and request assistance. More recently, Artificial Intelligence (AI)-driven traffic management systems facilitate monitoring, analysis, and optimisation of vehicle flows in real-time (Englund et al. 2021). Fusing data from different sources, such as traffic cameras, sensors, GPS, and connected vehicles, AI algorithms analyse traffic patterns, predict congestion, and dynamically adjust traffic signals or suggest alternative routes to drivers (Singh et al. 2021). Such systems could mitigate traffic congestion, improve road safety, and enhance the efficiency of the transportation networks (National Highways, 2024a).

While digital roads and related technologies offer the aforementioned benefits, data-driven systems raise significant concerns about the privacy of the road user (Paiva et al. 2020). Key issues include data security, informed consent, and the risk of data misuse as road user-information is collected, processed, analysed, and shared across multiple platforms and service providers (Walter and Abendroth 2020; Ljubi and Groznik 2023). This intertwining of technological advancements and privacy concerns necessitates a delicate assessment of the impact and challenges posed by the adoption of digital roads on users' privacy (Paiva et al. 2020). Ethical considerations should be prioritised when implementing these new technologies on road networks (Bonnefon et al. 2020).

The General Data Protection Regulation (GDPR) serves as the cornerstone for enhancing the protection of personal data across many European countries and regulates how organisations should handle and process such data (European Parliament 2016). However, new technologies pose a higher risk because of cybersecurity threats, data misuse by third parties, and the potential for biased decision-making by AI systems (Kleizen et al. 2023). Such threats, in turn, challenge GDPR's adequacy in guiding and regulating comprehensive data collection, storage and processing practices. Therefore, there is a pressing need to develop proactive regulatory frameworks and procedures within organisations. To develop a regulatory framework that effectively and dynamically accommodates the complexity of these new technologies, it is important to firstly understand road user concerns in this evolving landscape.

Much of the evidence thus far focuses on the implications of CAVs for user privacy, rather than digital roads, where CAVs may form part of a broader user-centred system of data collection and processing. This evidence is primarily drawn from insights by CAV experts, with comparatively less attention given to the road-user perspective and their concerns about such technologies (Liu et al. 2020; Olovsson et al. 2022; Acheampong et al. 2023). Empirical studies to date employ both qualitative (Islami et al. 2022; Rodwell et al. 2023) and quantitative methods, with the latter including survey questionnaires (Walter and Abendroth 2020; Ljubi and Groznik 2023) and discrete choice experiments (Potoglou et al. 2020; Boogert & Ding 2023).

Digital Roads introduce an additional layer of complexity, as multiple technologies – including CAVs and AI-driven intelligent transport systems – are increasingly integrated. In this context, and given prior research showing that privacy concerns may vary across countries and cultures (Patil et al. 2016a; Patil et al. 2016b; Potoglou et al. 2017), the aim of this paper is to examine the road-user perspective on 'Digital Roads', an ongoing initiative led by National Highways in the UK. More specifically, this study seeks to: (a) identify the key concerns of road users across a range of digital-road related technology adoption scenarios; and (b) explore the trade-off narratives expressed by road users when such technologies are implemented on Digital Roads.

The remainder of this paper is organised as follows. Section 2 presents a critical synthesis of the literature on users' privacy concerns and the trade-offs associated with digital technologies in road transport. Section 3 outlines the methodology employed in this study. Sections 4 and 5 present and discuss the study's findings, respectively. Section 6 concludes this paper and provides recommendations for future research.

2. Road-user privacy concerns and trade-offs: A critical overview

This section provides a critical overview of the definitions and types of road users' privacy concerns. It is also important to map the various trade-offs that affect road users' willingness to adopt new technologies, which may potentially threaten their privacy. This knowledge provides the foundation and context for a better understanding of the specific factors that road users consider when evaluating new transportation technologies.

As shown in Table 1, a synthesis of previous studies identified five privacy concerns in relation to new technologies: (1) the type of the personal information collected; (2) the level of control (or not) over data sharing with third parties; (3) the platforms through which data is shared; (4) the duration of data retention by the collecting organisation; and (5) the potential for data misuse by the collector and/or third parties. These concerns are discussed further in the following subsections.

2.1. Type of personal information

When managing transport infrastructure in the future, new technologies may be applied to collect a wide range of personal information, including time, location, speed data, CCTV footage, habit data and multimedia data. As new technologies – such as location-tracking/sharing smart apps, driving behaviour assessment systems and CAVs – continue to evolve, the collection of sensitive and large amounts of data poses significant concerns regarding the risk of identifying individuals and/or misusing their data. Such data may

Table 1
Privacy concerns related to new technologies and examples in the literature.

Privacy concern against	Explanation	Examples	References
Type of personal information	Types of data collected that may be sensitive to individuals	Speed, road facing camera, g forces, GPS data, driver-facing camera, time data, location data, habitual data, multimedia data	van den Boogert & Ding (2023); Patil et al. (2014); Picco et al., (2023); Ljubi and Groznik (2023); McCarthy et al. (2016)
Control over data sharing	The ability of road users to manage and control how their personal information is collected, used and shared by various services and platforms	No sharing; share with government, academic institutions, corporate organisations, societal organisations, transport authorities, police or law enforcement, security or intelligence agencies; ability to choose who to share data with	Picco et al., (2023);van den Boogert & Ding (2023); Patil et al. (2014); Ying et al.(2023); Chen et al. (2023) (Chen et al. 2023; Ljubi and Groznik 2023);
Data sharing platforms	Digital systems or services that facilitate the exchange, sharing, and management of data across various parties, such as individuals, organisations, and businesses	"Your location is sent to your emergency contacts via a social network account/ by email/by text message"	McCarthy et al. (2016)
Data retention duration	The period during which data is stored and maintained by an organisation or service before it is deleted or otherwise disposed of	Data not stored vs. data stored for different time intervals (days, months, years)	Potoglou et al. (2015); Patil et al. (2016b)
Potential data misuse	The improper or unauthorised use of road-user data by the collecting organisation or third parties	Information collected by service providers could be misused in various ways including location and movement tracking, location-based advertainments and fraudulent activities, and identification of individuals	Hunecke et al. (2021); Ljubi and Groznik (2023); Walter & Abendroth (2020); Ying et al.(2023); McCarthy et al. (2016)

include an individual's location at a given time (Ljubi and Groznik 2023; Ying et al. 2023), route movement (Rahimi et al. 2020), driving habits or other habitual data in the vehicle, such as entertainment or seating preferences (Ljubi and Groznik 2023), as well as public transport CCTV data (Patil et al. 2016b). As a result, road users worry that adopting new technologies will lead to excessive and unnecessary collection of their personal data (Chen et al. 2023).

2.2. Control over data sharing and data-sharing platforms

Road users often worry about how their personal data will be used or shared when considering the adoption of new technology. Their primary concern is the potential sharing or selling of their information to third parties (e.g., Picco et al., 2023; Ying et al., 2023). Therefore, knowing which entities have access to their data is important to them (Patil et al. 2016b; Boogert & Ding 2023; Picco et al. 2023; Ying et al. 2023). However, it is worth highlighting that prior empirical research has shown that individuals have different levels of tolerance for information sharing. For example, their willingness to disclose data may vary depending on whether the data will be shared with government agencies, academic institutions, business entities, societal organisations, travel authorities, or the police. Most importantly, obtaining road users' consent to share data (Potoglou et al. 2015; Chen et al. 2023), being transparent about who might be their data recipients and/or 'handlers', and offering them choices (Picco et al. 2023) are also critical factors in addressing road users' concerns.

Data-sharing platforms refer to digital systems or services that facilitate the exchange, sharing, and management of data across various parties. These platforms often determine the level of security, data access and usage policies, and overall protection of user information. A robust and secure data-sharing platform can instill confidence in road users by implementing encryption, authentication measures, and strict access controls. For example, a study by McCarthy et al. (2016) tested a personal safety app for reporting anti-social behaviour on public transport. The study found that people's likelihood of purchasing the app varied depending on the method of communication offered, such as sending location information to emergency contacts via social network accounts, email, or text messages.

2.3. Data retention duration

The length of time that data is stored is another key concern for individuals when it comes to data collection using new technologies in road transport (Potoglou et al. 2015; Patil et al. 2016b). If road users know that their data will be retained for a long period, they may be more cautious about what they disclose or even reluctant to share sensitive information. For example, Patil et al. (2016b) conducted a choice experiment involving CCTV camera data for security and surveillance checks at train and metro facilities in 27 European countries. The study revealed that different data retention durations resulted in varying levels of preference for security and surveillance options. The results also showed a U-shaped pattern: a storage time of 15 days was the most preferred, followed by 7 days and 3 days, while a storage time of 45 days was the least preferred. This suggests that road users prefer shorter storage times and become more cautious as storage time increases.

2.4. Potential for data misuse

Another road-user concern relates to the misuse of their data (Walter and Abendroth 2020; Ljubi and Groznik 2023), which involves the unauthorised or inappropriate use of their personal information. Misuse can take various forms; for example, tracking road users' locations (McCarthy et al. 2016) or routes (Ljubi and Groznik 2023), identifying individuals (Ying et al. 2023), or using location-based data for targeted advertising or fraudulent activities (Ying et al. 2023). Road users are also concerned that processing or unauthorised access to their sensitive data may result in other unforeseen issues (Walter and Abendroth 2020).

To alleviate road users' concerns about data misuse, technology and service providers need to be transparent about the purpose of data use. For example, driving monitoring devices use driving data from car users to provide them with driving feedback (Picco et al. 2023). Similarly, CCTV data from subway or train stations is used by police for security and surveillance checks (McCarthy et al. 2016).

2.5. Trade-offs between data sharing and perceived benefits

When deciding whether to adopt a new technology, road users typically make a trade-off between sharing their personal data and the benefits that come with it (Cottrill and Vonu Thakuriah 2015). This aligns with the privacy calculus theory, which suggests that an individual's data self-disclosure behaviour or intention is based on a cost-benefit analysis weighing potential risks and advantages (Culnan and Armstrong 1999). Previous privacy-related literature has identified the following four trade-offs that road users typically consider regarding data privacy risks associated with adopting new technologies in the transportation sector (as shown in Fig. 1). These include monetary incentives, usability, and security of the technology, and the environmental benefits the technology may bring.

The first type of trade-off in transportation is between monetary incentives and data privacy, where road users are generally willing to accept monetary incentives or discounts in exchange for disclosing their personal data (Hunecke et al. 2021; Boogert and Ding 2023). The second type of trade-off is between the usability of the new technology and data privacy. For example, road users tend to weigh the benefits of enhancements – such as improved parking (Walter and Abendroth 2020), traffic management (Ljubi and Groznik 2023), driving assistance (Rahimi et al. 2020), location-based recommendations (Ying et al. 2023) – against concerns about their data privacy, as most of these technologies offer them more convenience, efficiency and time savings.

Safety is another important consideration in transportation (McCarthy et al. 2016; Patil et al. 2016b; Picco et al. 2023). For

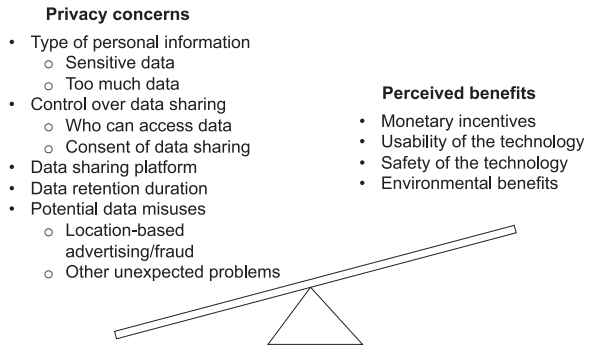

Fig. 1. Trade-offs in users' adoption of new technologies in the road transport sector.

example, the disclosing data for automated and assisted driving technologies can improve travel safety (Picco et al. 2023). In addition, environmental benefits are a key consideration for road users, especially with automated and assisted driving technologies, as these can reduce fuel consumption and emissions by optimising driving behaviours and enhancing traffic flow (Rahimi et al. 2020; Chen et al. 2023).

When road users weigh privacy concerns against perceived benefits, they tend to prioritise certain concerns over others (Patil et al. 2016b). For example, a study on health data storage revealed that patients placed greater importance on who could access their data rather than the specific types of personal information being stored (Patil et al. 2016a). Additionally, there were significant differences in individual privacy preferences across nations, cultures, and socio-economic characteristics (Potoglou et al. 2017). Therefore, the objectives of this study are: (a) to capture road-users' privacy concerns about digital roads and (b) to explore their narrative trade-offs against perceived benefits (e.g., safety, timely response to incidents) when new technologies are implemented in the context of the 'Digital Roads' initiative.

3. Materials and methods

To achieve the objectives outlined in Section 1, this study designed and conducted a series of workshops, which were guided by several scenarios within the context of the 'Digital Roads' initiative in the UK (National Highways 2021). The research design consisted of three distinct stages: the study design, data collection, and thematic analysis (see, also Fig. 2).

3.1. Design of the scenarios

Three scenarios were developed based on new technologies likely to be implemented by National Highways on the UK's motorways in the future. These scenarios covered various technologies, providing participants with practical, real-world contexts. As a result, participants were able to offer more nuanced and authentic feedback, reflecting their concerns, questions, and suggestions related to data sharing and the three scenarios involving the adoption of digital road technologies.

Specifically, the three scenarios involved innovative and data-related technologies: (a) Artificial Intelligence (AI)-based capturing of images of drivers who exhibit 'bad' driving behaviours ("Bad Driver Behaviour"), (b) "Connected Vehicles", and (c) "Dynamic Signalling and Stopped Vehicle Detection". Detailed descriptions and illustrations of each scenario are presented in Fig. 3.

3.1.1. Scenarios 1A and 1B: Two scenarios of "Bad driver Behaviour"

The UK transport sector recently trialled 'sensor test van' technology on motorways, which involves installing smart cameras in stationary vans at the side of the road (National Highways 2022). These cameras are supported by AI and can capture images of drivers engaging in unsafe behaviours, such as not wearing seat belts, smoking, eating, using their phones, or speeding. Drivers who are caught violating these rules would receive a 'warning letter' from the police and may face fines of up to £500. The aim of this technology is to help regulate and reduce bad driving behaviour among drivers (National Highways 2022).

Drawing from this trial, this study developed a scenario that focused on bad driving behaviours. The scenario assumed that the data collected through this technology could include images of both the driver and the vehicle, the vehicle's registration number, additional details,[1] and the vehicle's location. To gain a deeper understanding of road users' perspectives, this scenario was divided into two sub-scenarios: Scenario 1A (see Fig. 3) in which participants observed other drivers displaying bad driving behaviours; and Scenario 1B in which participants were the drivers themselves engaged in these behaviours.

3.1.2. Scenario 2: The "Connected Vehicles" scenario

To improve communication between road infrastructure and users, the UK's National Highways is planning to deploy infrastructure

[1] This term was intentionally introduced as a non-specific data collection process in order to capture participants' reactions.

Fig. 2. Study design, data collection, and thematic analysis.

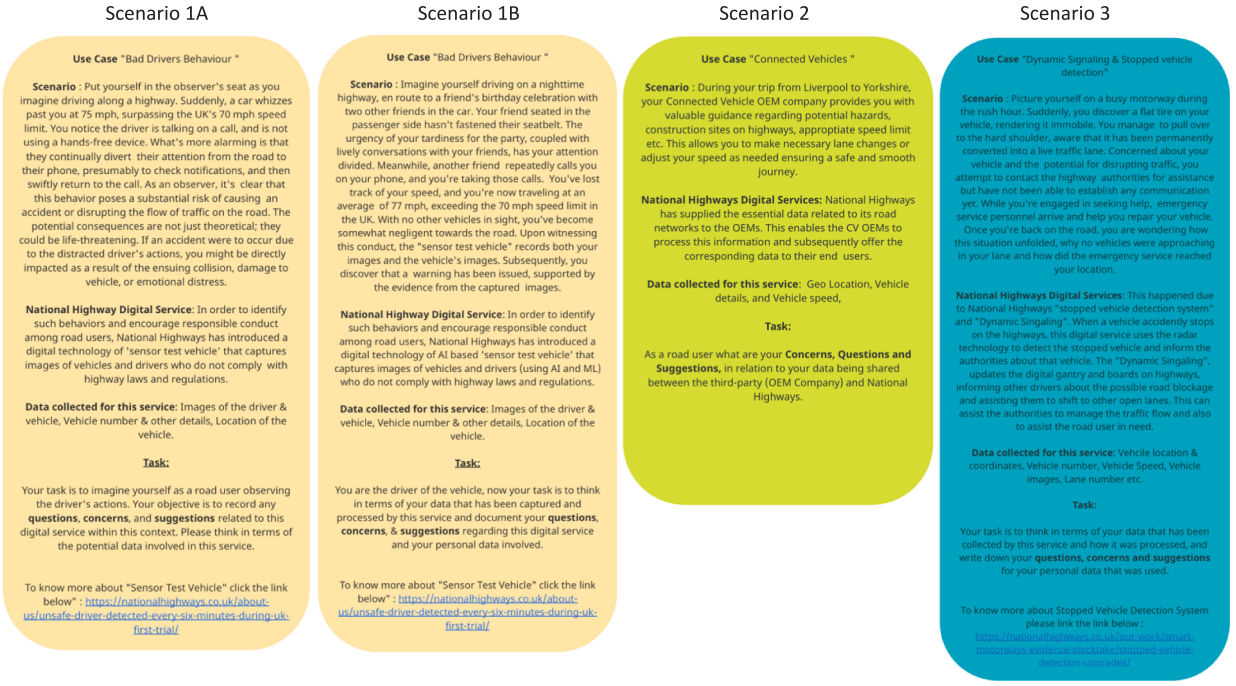

Fig. 3. The hypothetical scenarios presented in the workshops.

to facilitate Connected Vehicles (CVs) in the future. CVs can wirelessly communicate and exchange information with other vehicles, external networks, and infrastructure using technologies such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), and Vehicle-to-Everything (V2X) (Liu et al. 2020).

In this study, the "Connected Vehicles" scenario was designed to enable real-time communication, including the exchange of real-time information such as routes, incidents, upcoming road construction, and journey details, displayed on the vehicle's in-car panel (see Scenario 2 in Fig. 3). The scenario assumed that the data collected through this technology could include the vehicle's location and coordinates, registration number, speed, and images.

3.1.3. Scenario 3: The "Dynamic signalling and stopped vehicle Detection" scenario

The transport sector is also in the process of implementing stopped vehicle detection using radar-based technology nationwide (National Highways 2024b). These radar devices will be installed along the roadside to detect stopped vehicles. This scenario was also included in our study. When a vehicle is detected, operators in the control room can view images of the incident, close lanes or adjust speed limits as needed, and dispatch traffic police to handle the stopped vehicle (see Scenario 3 in Fig. 3). The scenario assumed that the data collected through this technology could include the lane number, location and coordinates, number, speed, and images of the vehicle.

3.2. Workshops

The scenarios shown in Fig. 3 were designed for a series of workshops conducted both online and in-person. Each workshop began with an introduction to the 'Digital Roads' initiative by NH and the objectives of the research (see Appendix A1 for details on how the scenarios were introduced to participants). Participants were then presented with each of the three scenarios in the order shown in Fig. 3 and were asked to imagine themselves as being the drivers experiencing these situations.

The scenarios were in turn displayed on Miro,[2] an online collaboration platform, allowing participants to read, review and directly type their feedback. A facilitator from the research team provided clarifications and instructions while participants reviewed the scenarios. Each participant had approximately 10 min to review each scenario and note their concerns, questions, and suggestions about the data collection, processing and the technologies involved using colour-coded sticky notes on Miro (see Appendix: Figs. A2 and A3 for instructions and an example scenario presentation, respectively). The research team organised a total of five workshops: four online and one in-person. Each workshop lasted approximately one hour.

3.3. Recruitment of participants

The data collection involved 20 participants and was conducted between November 2023 and January 2024. Table 2 summarises the key characteristics of the participants. Among them, 18 were from academia (graduate students or researchers), including seven experts in cybersecurity, computer science, business, and transport planning. The remaining two participants were professionals working in the transport sector. Although all participants were asked to view the scenarios as a regular road user, their specialist knowledge enabled the collection of insights from both road user and expert perspectives relevant to privacy and new road transport technologies. The sample size adhered to the general guidelines for qualitative research and reached data saturation, thus supporting the reliability of the findings and providing adequate evidence for the subsequent thematic analysis (Creswell 1998; Guest et al. 2006).

3.4. Thematic analysis

Concerns, questions, and suggestions reported in the workshops were collated and grouped using thematic analysis, a widely used technique of qualitative data analysis in transport and mobility research (e.g., Liu et al. 2020; Song and Potoglou 2024). The aim was to explore the concerns and levels of trade-offs (benefits vs. concerns) across scenarios. The analysis of the workshop responses involved two main stages: data-driven coding and theme identification (Braun and Clarke 2006).

Firstly, data-driven coding was based on the raw quotations from participants rather than the researchers' own impressions or interpretations of the responses (Maguire and Delahunt 2017). This approach ensured that participant perspectives were captured accurately. The manual coding process involved repeated readings of the participants' sticky notes and meticulous note-taking to identify relevant codes. Privacy concerns identified in Section 3, such as "types of data" and "control over data," guided the selection of coding labels. Participants used different coloured-coded sticky notes to categorise their responses across questions, concerns, and suggestions. However, for the purposes of data-driven coding in this analysis, all responses were thoroughly screened to identify concerns related to new road technologies.

Secondly, codes derived from the data-driven coding exercise and their related extracts were organised into overarching themes. This organisation aimed to ensure that the final thematic map aligned with the study's research objectives. The identified themes provided a structured framework to understand and interpret the data, highlighting common patterns and key issues raised by participants (Adams 2015).

4. Findings: Road user trade-offs and concerns

As presented in Table 3, the analysis of the workshop data showed that participants primarily weighed the balance between travel safety and data privacy in Scenarios 1 and 3. In contrast, in Scenario 2, participants focused on the trade-off between the usability of connected vehicle technology and data privacy. This suggests that when considering Scenarios 1 and 3, participants prioritised safety, whereas for Scenario 2, usability of new technologies took precedence.

As shown in Fig. 4, the thematic analysis of the data revealed six core themes related to road users' concerns: (1) privacy; (2) technology; (3) data security; (4) awareness; (5) consequences; (6) third-party use. These themes further included a variety of sub-

[2] https://miro.com/app/dashboard/.

Table 2
Workshop participants.

Respondent	Gender	Role	Background	Workshop mode
P1	Female	Academic expert	Cyber Security	Online
P2	Male	Academic expert	Computer Science	Online
P3	Female	PhD student	Business	Online
P4	Female	Academic expert	Computer Science	Online
P5	Male	Academic expert	Business	Online
P6	Female	PhD student	Geography Planning	Online
P7	Male	Industry expert	Transport sector	Online
P8	Male	Industry expert	Transport sector	Online
P9	Male	Academic expert	Geography Planning	Online
P10	Male	Master's student	Computer Science	In person
P11	Male	Master's student	Computer Science	In person
P12	Male	Master's student	Computer Science	In person
P13	Female	Master's student	Computer Science	In person
P14	Male	Master's student	Computer Science	In person
P15	Male	PhD student	Geography Planning	In person
P16	Male	Master's student	Computer Science	In person
P17	Male	Master's student	Computer Science	In person
P18	Male	Master's student	Computer Science	In person
P19	Male	Master's student	Computer Science	In person
P20	Male	Master's student	Computer Science	In person

Table 3
Trade-offs and corresponding quotation examples across the Scenarios.

Scenario	**Trade off**	**Quotation example**	**Freq. of responses**
1a. Bad driver behaviour (other people)	Travel Safety – Data Privacy	*"I don't have concerns about bad drivers' data being collected. As long as it offers better safety on the road"*	3
1b. Bad driver behaviour (participant)	Travel Safety – Data Privacy	*"Difficult ethical dilemma – private data via road safety. Could we ensure road safety without collecting large amounts of private data?"*	4
2. Connected vehicle	Usability – Data Privacy	*"Info on nearby speed cameras is useful"* or *"Does the data actually improve the journey?"*	2
3. Dynamic signalling and stopped vehicle detection	Travel Safety – Data Privacy	*"This application is not one based on trying to change driver behaviour but to respond to a possible emergency – this feels a better use of tech. Immediate danger as opposed to possible danger"*	2

themes raised by participants, providing insight into their perspectives and priorities regarding the adoption of new transportation technologies. The analysis also showed that some sub-themes overlapped, with a few quotes supporting multiple themes. These overlaps and complexities were retained in Fig. 4 to accurately reflect the data and to guide the discussion of the findings in the following subsections.

4.1. Privacy concerns

As shown in Fig. 5, six sub-themes of road users' privacy concerns were identified from the workshop data: (1) type of data, (2) share with whom, (3) control over data, (4) data misuse, (5) data-retention duration, (6) data-sharing platforms.

4.1.1. Type of data

In all three scenarios, participants consistently expressed a desire for transparency regarding the collection of vehicle data and personal information. For example, they frequently asked questions such as, "What vehicle details are collected?" (Participant (P) 4, Scenario (S) 2) or "What kind of data did they collect from me?" (P3, S3).

Participants were also curious about the scope of the data collection. Many were uncertain whether the data collection applied to all drivers or only those exhibiting bad behaviour, whether passenger information would be collected, and the timeframe for data collection. Some of their specific questions included:

"In order to identify bad drivers, does it collect data about all drivers?" (P2, S1A).

"Is it just driver data that is captured?" (P7, S1A).

"Will my passengers be captured as well?" (P9, S1B).

"Is this data collected all the time, or just during an incident?" (P8, S3).

Participants expressed concerns regarding the extent of location data collected:

"I have no concerns with location data where this happens, but it's unclear how much of it is collected, ie. would the system know where the driver is coming from? or just where they started going over the speed limit?" (P4, 1A).

In addition, participants perceived certain types of data – such as images (P6, S3), personal preferences (P3, S2), vehicle numbers

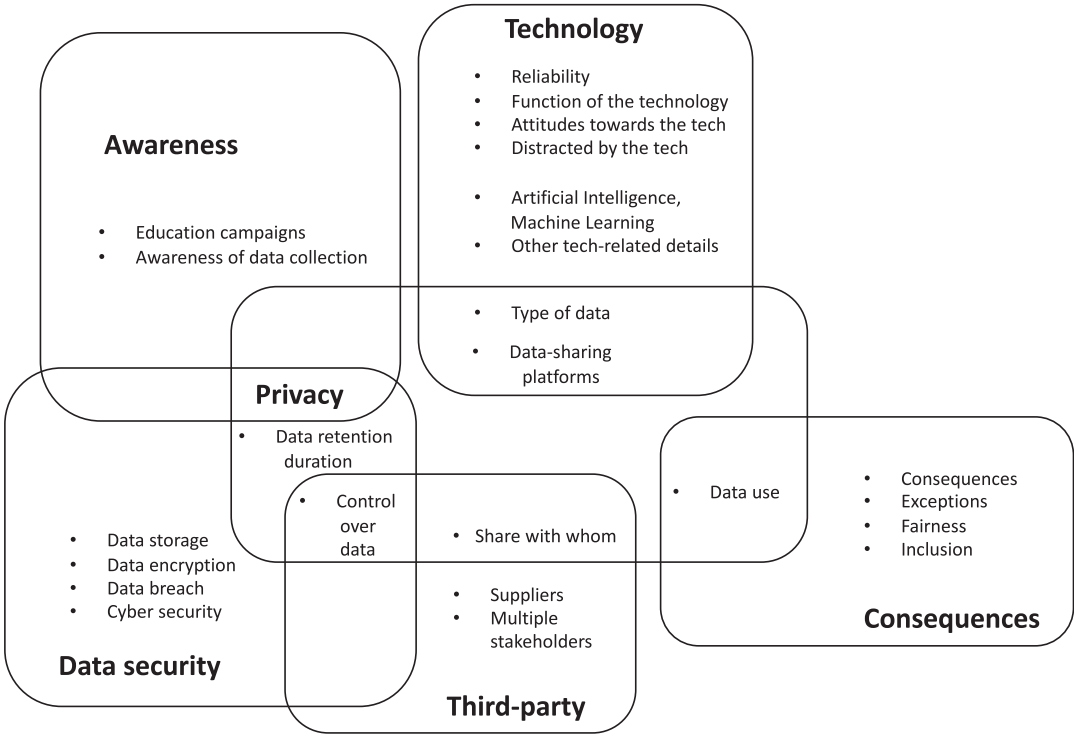

Fig. 4. Thematic analysis of road users' concerns about the adoption of new technologies.

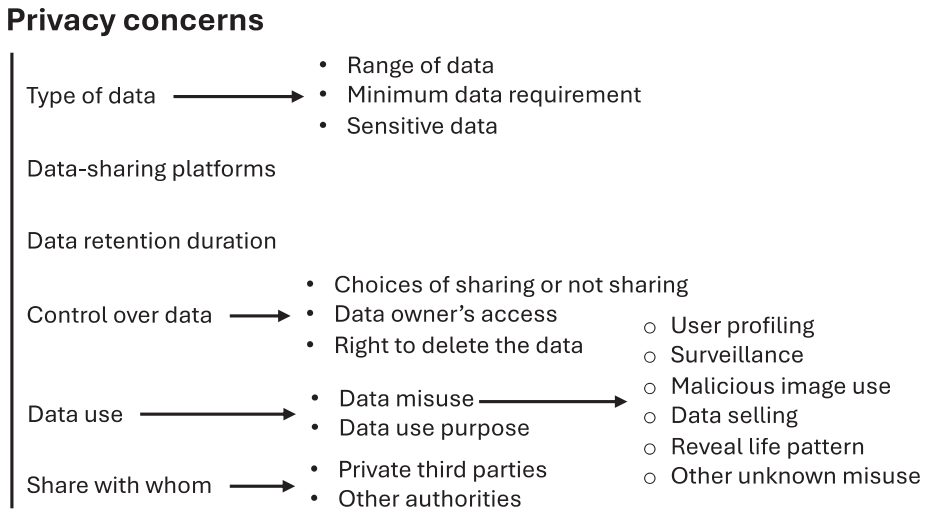

Fig. 5. Sub-themes identified regarding road users' privacy concerns.

(P4, S3), and locations (P16, S2) – as more sensitive. They expressed concern that these data could be misused or leaked.

"Why the image data is needed? How it will be used? Is there a risk of image data misuse and leakage?" (P6, S3).

"OEMs [Original equipment manufacturer] have a lot of information about their customers, including behaviours, and attitudes. Even things such as the songs I listen to while driving and the volume levels. is all this data used between the third party and NH?" (P3, S2).

"Is this data used just to provide assistance and manage traffic, or would it be shared with any 3rd parties? If that's the case, then vehicle number maybe shouldn't be shared?" (P4, S3).

"Geo-location can actually give people an idea of my daily/weekly movement in the case of a data breach, which is dangerous." (P16, S2).

"Will I be able to know on which road or networks I am being tracked?" (P14, S3).

4.1.2. Share with whom

Participants were primarily concerned about who would have access to their data. They wanted to know whether the data would be collected directly by the transport sector and whether it would be shared with other departments – such as traffic enforcement agencies or the police – for purposes like identifying traffic violations or other criminal activities.

"Could images be shared with other authorities? e.g. to identify criminals or illegal immigrants using face recognition?" (P1, S1A).

"Why my images are taken? Will it be shared with the traffic enforcement agency? How it will be used for my pictures? (P6, S1B)".

Participants were also concerned that their data might be shared with unknown third parties, including car insurance companies, advertisers, and emergency services. Consequently, they were eager to understand how their data would flow and be managed.

"Is my data collected by a third party or is it collected by NH and shared with a third party?" (P3, S2).

"I'm concerned that the data can be used directly by insurance companies. This is concerning because it would mean that insurance companies would force people to become restrained and repressed by the law. (P19, S1A)".

"Main concern if data becomes available to insurance companies – e,g, some vehicles brake more often and hence the insurance will go up. (P1, S3)".

In addition, participants expressed clear distrust of private third parties managing their data. They were concerned that involving third parties could increase the risk of data being sold without consent, personal preferences and user profiles being compromised, and vulnerability to cyberattacks.

"This brings us to the question of sharing personal data with third party. In case of a supply chain attack, this could be a disaster. (P16, S2)".

4.1.3. Data-sharing platforms

The availability of data-sharing platforms was also important for road users. Participants expressed a desire to access information about how their data was collected and used. They wanted to know whether there were any communication channels through which the transport sector could keep them informed, such as in-vehicle display boards, text messages to mobile phones, highway notice boards, or notifications after a traffic violation.

"What are the options for road users to learn about how their data is used and who is it shared with? What clear and easy-to-use ways of seeing info about the use and sharing of data exist?" (P1, S1A).

"How is the corresponding data offered to end users? In the form of mobile notifications, Motorway board warnings?" (P13, S2).

4.1.4. Data retention duration

Participants also wanted to know how long their data would be retained by the collecting organisation. They expressed concern that the data might be stored longer than initially stated or used for purposes beyond the original intent. This worry about data retention reflects a deep unease regarding transparency and trust in how organisations manage personal information, as well as a desire for control over the duration and purpose of data storage.

"How will it impact us if we are near the bad-behaviour driver? As this record will be saved for longer purposes as evidence. (P12, S1A)".

"Will this data be stored forever?" (P18, S1B).

4.1.5. Control over data

Having control over their own data was important to road users. They expressed concerns about the lack of choice in deciding whether to share their information and about the consent process for data collection (P3, S1A), fearing that data sharing might be mandatory (P9, S1B).

"Can I opt-out of my data being collected? (P3, S1A)".

"If NH doesn't have consent from passengers, how this data will be dealt with in legal matters?" (P9, S1B).

They therefore emphasised the importance of having access to their data and understanding how it is used. They believed that they had the right to request access to their data and to have their information deleted.

"I would like the data path to be clear for the data owner. I mean, I would like to know who has been able to access my data, when and for what reasons." (P14, S1A).

"As the data owner, do I have right to ask that my information be deleted after use." (P16, S1A).

4.1.6. Data use purpose and data misuse

Participants expressed concerns about data use, in two main areas. Firstly, they felt that the purpose of data collection was not clearly explained, often questioning about why their data was being collected in the first place. Secondly, they perceived a high risk of data misuse due to this lack of transparency regarding the purposes of data collection.

For example, for Scenarios 1A and 1B ("bad driver behaviour" scenario), participants were unsure if the data would be used for police enforcement. In Scenario 2, ("connected vehicle" scenario), participants questioned the necessity of collecting data beyond location and speed, especially if the purpose was limited to providing "general updates on construction and hazards" (P4, S2). In Scenario 3 ("dynamic signalling and stopped vehicle detection" scenario), participants were concerned whether data would be shared with third parties even if the stated purpose was to "provide assistance and manage traffic" (P4, S3).

These unclear purposes of data use raised concerns about various potential risks, including user profiling (P19, S1A), surveillance (P11, S1B), malicious use of image data (P1, S1B), unauthorised sale of data (P18, S2), disclosure of lifestyle patterns (P7, S1A), and other unforeseen risks (P3, S1A).

"Is the gathering structured to create user profiles?" (P19, S1A).

"I'm concerned about whether the system could be used for surveillance beyond the road traffic issue. It could be used to track people down with political purposes. Big brother like." (P11, S1B).

"That images will be used maliciously" (P1, S1B).

"I'm concerned that the service will constantly try to record the maximum on each user for business purposes" (P18, S2).

"For what other purpose could my data be used? Could NH reveal my pattern of life?" (P7, S1A).

"Does NH use this data beyond this application? I feel like my data in all forms is being manipulated for their own improvements and processes." (P3, S1A).

4.2. Technology concerns

Fig. 6 identifies five sub-themes related to technology concerns, including: (1) specific technologies (Machine Learning, Artificial Intelligence); (2) other technology-related details such as why the technology is being used and how the data are collected, (3) the function of the technology (e.g., reliability, timeliness); (4) distraction caused by the technology; (5) attitudes towards the technology.

4.2.1. Artificial Intelligence and Machine learning technologies

Participants expressed clear concerns about specific technologies, such as AI and machine learning (ML). One major issues was the transparency of AI training; participants voiced reservations about the sources of training data and the duration of the training process. Another concern focused on the operation of AI, particularly regarding the potential for errors and bias.

"What is done about false positives and how can false negatives be recorded?"(P10, S1A).

"The statistics are heavily skewed in the link [https://nationalhighways.co.uk/about-us/unsafe-driver-detected-every-six-minutes-during-uk-first-trial/] towards Male 30–49-year-olds. Does this mean this demographic is more likely to be picked up by the AI than other demographics? How can you know?" (P15, S1A).

Participants believed that human or AI supervision during both the training and operational phases is important to minimise AI errors and validate results, especially when detecting poor driving behaviours.

"Who is going to be evaluating the data, either a human or an AI system?" (P12, S1A).

4.2.2. Other technology-related details

Participants were curious about the reasons for adopting new technologies over traditional solutions. For example, in Scenario 3, some participants questioned the functional differences between the proposed technology and the hard shoulder. In Scenario 2, one participant suggested that existing technologies, such as satellite navigation, might already serve a similar purpose raising questions about the need for further development. Similarly, in Scenario 1, participants questioned whether the new technology was superior to existing solutions such as traditional speed cameras.

They also wanted a clear understanding of how the new technology would be used for data collection. For example, in Scenario 1, participants wanted to know how the technology differentiates between identical people (P17), how detection would be triggered (P5), how trustworthy the sensors are (P11), and how people's permission for data collection would be obtained (P17). In Scenario 2, participants were interested in how frequently construction or hazard data would be updated (P4). In Scenario 3, they wanted to know how accurate the technology is (P14), how it distinguishes between emergencies and normal stops (P16), and how the information would be shared with road users—through mobile notifications or motorway board warnings (P13).

4.2.3. The function of the technology

Potential errors or biases in AI training and operation led participants to question the technology's functionality, including

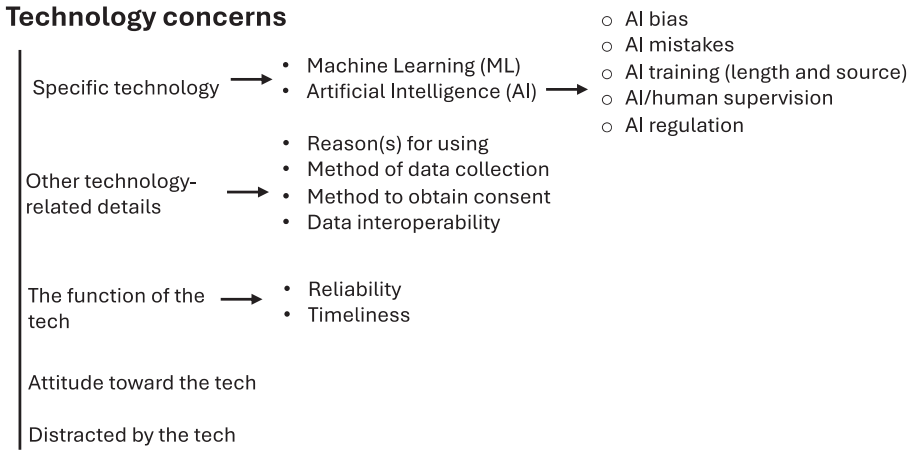

Fig. 6. Sub-themes regarding road users' technology concerns.

concerns about its reliability, accuracy, and timeliness. These factors, in turn, greatly influenced participants' trust in the technology.

"Main concern is reliability and timeliness of the data" (P4, S2).

"If this technology is not accurate enough, it may detect the wrong person and also miss the one who is speeding." (P6, S1A).

"Can I trust the data?" (P8, S2).

4.2.4. Road users' attitudes towards the technology

While objective factors related to technology – such as accuracy, reliability, and data collection methods – are important for road users when deciding whether to adopt new technologies, personal attitudes also play an important role. Participants expressed a range of emotions towards technology, from scepticism to acceptance, which profoundly influenced their willingness to engage with these innovations. Several participants expressed discomfort with the prospect of technology overly controlling or manipulating their behaviours. For example, one participant expressed concerns about surveillance, stating:

"This is feeling a bit too heavy-handed in terms of the use of tech to shape behaviour." (P5, S1B).

4.2.5. Distracted by the technology

Concerns about distraction caused by new technologies emerged as an important theme among participants. Many feared that the presence of monitoring systems could divert their attention away from the road, potentially leading to unsafe driving behaviours. One participant expressed this concern as:

"I'm concerned that I'd become too distracted with avoiding the Sensor that record what I am doing." (P18, S1B).

4.3. Data security concerns

Four sub-themes of data security-related concerns were identified in Fig. 7: (1) data storage, (2) data encryption, (3) data breach, and (4) cyber security.

Data security is a key concern for road users. Participants emphasised the importance of data encryption due to worries about the malicious use of non-anonymised images (P1, 1B) and the potential for personal identification (P7, S2).

"How secure is this data? can it be modified by a malicious actor (i.e. make it seem less traffic on one route and cause blockades)?" (P14, S2).

Concerns about the consequences of data breaches were also prevalent. One participant was particularly worried that their daily/weekly whereabouts could be revealed if geolocation data were compromised (P16, S2).

With the potential implementation of future connected vehicle technologies (Scenario 2), many cybersecurity concerns emerged among participants, including fears of cyberattacks tampering with data (P9), malicious modification of data by bad actors (P14), and supply chain attacks involving third-party data collectors (P16).

Participants also expressed concerns about the physical location of data storage, preferring segregation and local storage within the system to ensure data security (P18, 1B). Additionally, they sought clarity on how data is stored and processed, emphasising the need for secure procedures (P7, S1A). Participants also expressed the right to choose their data storage suppliers by themselves (P14, S1A).

"The system should be isolated, detect if the users are misbehaving and alerting them further down the road. It should not be stored anywhere else than on the local system." (P18, S1B).

"How is the data stored and processed. Is it secure?" (P7, S1A).

"Will the data storage system be publicly owned or privatised? If it's privatised, will I be able to choose which provider manages my data?" (P14, S1A).

4.4. Awareness concerns

Two sub-themes of awareness-related concerns were identified in Fig. 8: (1) whether there would be measures to raise road users' awareness of data collection, and (2) education campaigns beforehand.

It is important for road users to be informed beforehand about any activities involving data collection. For example, participants

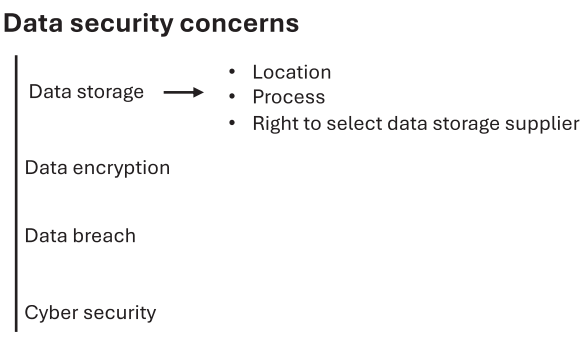

Fig. 7. Sub-themes identified around road users' data security concerns.

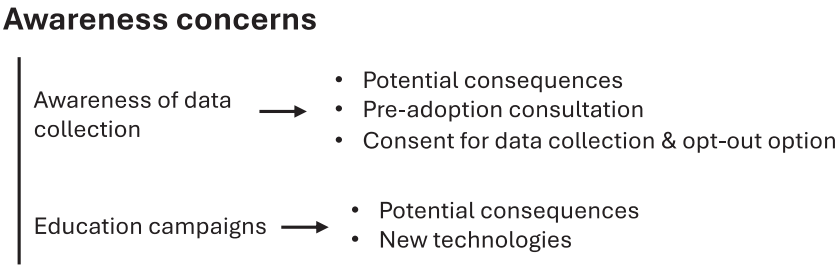

Fig. 8. Sub-themes identified around road users' awareness concerns.

may feel it is unfair to face penalties without prior notice that their driving data would be collected for traffic enforcement (P3, 1A/1B). Additionally, participants emphasised the importance of obtaining consent for data collection and the need to provide an opt-out option (P2, S2).

"If I do not know that my data is being collected and how and why it is being used, I think it is unfair that I should be penalised for anything. My consent matters to me." (P3, S1A/S1B).

Participants also recommended that road users be consulted prior to the adoption of new technologies (P1, S1A).

"Who decides if this service will become available? Do road users have a chance to vote or express their opinion about this? Are road users being asked?" (P1, S1A).

"I would suggest users are informed and mass awareness carried out on the need and use, also areas of identification and where it will be used (what parts of the road)" (P17, S1A).

At the same time, educational campaigns were recommended as an effective tool to raise road users' awareness about the ethical use of data in new technologies.

"Again, are there going to be educational campaigns to let drivers know about the new technology and the possible consequences of not following the rules." (P14, S1B).

4.5. Consequence concerns

Four sub-themes of consequence-related concerns were identified in Fig. 9: (1) the consequences arising from adopting the technology; (2) exceptions to these consequences; (3) fairness; and (4) inclusion when applying these consequences.

4.5.1. Consequences

Road users are concerned about the consequences of data collection, which are partly related to the purpose of collecting this data. Participants were worried about the possible negative outcomes of adopting the technology. For example, participants in Scenario 1 were concerned about the uncertainty surrounding the consequences of bad driving behaviour. These concerns included possible legal repercussions such as prosecution or fines (P1), impact on driving records (P3) or increases in insurance premium rates (P19, P14). They also feared that the data collected could be used to humiliate individuals who violate regulations, potentially damaging their reputations (P13, P1, P18).

Another concern related to penalties – participants questioned, for example, whether penalties would be determined solely based on the data (P12), whether the penalty system would be properly designed with varying severity (P8), or whether there would be a single, unified penalty for diverse violations (P3). Also, they questioned about penalties being unfairly applied to individuals using someone else's vehicle (P3, P4), and the responsibility of drivers vs. passengers for bad behaviour (P8, P11).

Some participants viewed data collection as a form of enforcement (P19), and preferred encouraging the use of certain technologies rather than imposing restrictions (P18). Conversely, one participant (P8) felt that consequences were necessary; without them, the

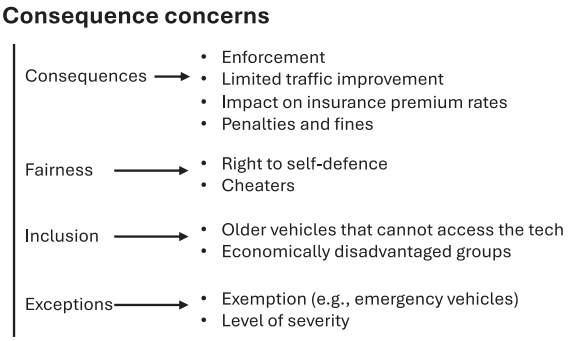

Fig. 9. Sub-themes of road users' concerns regarding consequences.

implementation of the technology would lose its meaning.

"People should be encouraged to do what's right. drivers are too often reminded to live in fear instead." (P19, S1A).

"If we are deploying tech to catch people doing dangerous things, at the cost of privacy, there should be actual consequences otherwise what is the point?" (P8, S1B).

In Scenario 2, one participant was concerned that sharing information might cause all road users to respond in the same way, potentially creating "unintended pressure on side roads, and disproportionately affect small communities" (P12). However, in Scenario 3, participants were concerned that failing to share data could result in delays across the road network, possibly leading to penalties (P3).

4.5.2. Exceptions

Exceptions need to be clearly defined when using collected data for traffic enforcement. For Scenario 1, exceptions include emergency calls (P9), the presence of emergency vehicles (P15), or speeding due to emergencies (P4, P15, P17). For Scenario 2, that includes unforeseen circumstances, such as a lack of internet connection (P4) and for Scenario 3, exceptions involve situations where a stop is normal rather than an emergency.

"What happens if you had a legitimate claim (such as emergency), what effects would that have on day to day life and how easy would they be to dispute/remove?" (P15, S1B).

"Even if it's coming from NH, how frequently is it updated? what if there's no internet connection?" (P4, S2).

"What if it wasn't an emergency but they needed to stop?" (P13, S3).

4.5.3. Fairness

In Scenario 1, participants emphasised fairness in terms of the consequences of the data collection. Some participants expressed concern that car drivers might use fake seat belts or alter their behaviour only when within the camera's field of view (P3, S1B). Participants therefore hoped that they would have the right to self-defend themselves if they encountered any errors or unfair treatment.

"I know there are clips that one can use to latch into the seatbelt and not wear a seatbelt. In that case. What will you do about that?" (P3, S1B).

"Many drivers know the exact places where cameras are located and hence are clever enough to 'game' them and not follow any rules where they know there are no cameras. How will this prevent me from doing this again?" (P3, S1B).

"Can I challenge the authorities that have issued me with this warning? based on that data" (P3, S1B).

4.5.4. Inclusion

In Scenario 2, participants expressed concerns about whether the technology considers the needs of all road users and ensures equitable access. They highlighted the importance of providing alternatives (P2, P14), particularly those using older vehicles that cannot access the latest technology (P18, P4), as well as economically disadvantaged groups (P5, P14).

"Because the data is coming 'from the car', there will be lots of cars who may not have that information – what's the utility of it then?" (P4, S2).

"Is there money to be made out of this and will it exclude some drivers." (P5, S2).

"Maybe this data could be readily available via displays instead of just to road users who can afford it" (P14, S2).

"Provide an option to redownload potential hazards, etc for my trip, so then no live data collection is needed." (P2, S2).

4.6. Third-party concerns

Two sub-themes of third-party concerns were identified in Fig. 10: (1) suppliers and (2) multiple stakeholders.

4.6.1. Suppliers

In the connected vehicle scenario (Scenario 2), participants raised concerns about third-party technology providers and their eligibility to collect data (P17). Additionally, they questioned whether they would have the freedom to choose their own data supplier (P15).

"Does the OEM have the right infrastructure to handle the data?" (P17, S2).

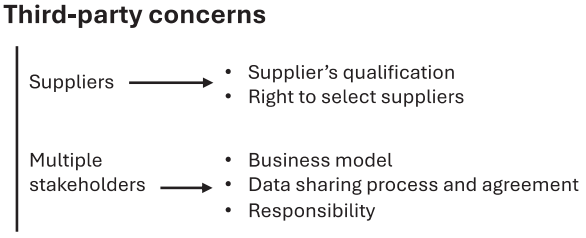

Fig. 10. Sub-themes identified around road users' third-party concerns.

"If I am forced to have a company. The government should provide an environment in which it is possible for player can enter OEM business, so I can have several options to choose." (P15, S2).

4.6.2. Multiple stakeholders

Participants expressed strong concerns about situations involving multiple stakeholders, particularly regarding the data-sharing processes and agreements between them (P5, 1A). They also questioned the commercial motivations of third parties, and the role of the transport sector in these engagements (P5/P7, S2). At the same time, participants were uncertain about who would be responsible for the technology (P6, S1A), who would regulate third parties (P3, S2), and who would address data leakage (P3/P6, S2).

"I think it is important to explore National Highways' role in terms of the involvement of third party. If National highways does not engage with customer data directly, how to ensure the third party use the data ethically? The responsibility of data misuse or leakage should be considered." (P6, S2).

"What is the threshold for using information collected to inform other agencies?" (P5, S1A).

"Is this a commercial motivation for NHs. I.e. to what extent should they be competing with other businesses in this space – what is their role?" (P5, S2).

"How is the company profiting from this, are they gathering my data?" (P7, S2).

5. Discussion

The aim of this study was to explore road users' concerns within the context of the 'Digital Roads' initiative focusing on the collection of road-user-related data and the potential risks associated with the collection, storage and sharing of such data through various new technology scenarios. These risks were identified through a series of workshops involving both road user and experts, guided by a set of hypothetical yet realistic technology-related scenarios. A key strength of this study lies in the use of these scenarios, which provided participants – especially those with limited prior knowledge – with a clear and practical understanding of how future technologies might be employed to collect traffic, vehicle and personal data. As a result, participant responses more accurately

Table 4
Comparison of findings with previous studies on privacy concerns of CAVs.

Country	Sample	Methods	Concerns	In favour (+) / Not in favour (−) to trade-off between privacy and…	Authors
UK	20 road users	Workshops	• Data privacy • Technology • Data security • Awareness of data collection • Consequences of data collection • Involvement of third parties	• Usability of the new technology (+) • Travel safety of adopting the new technology (+)	This study
Sweden	17 road users	Semi-structured interviews	• Comfort with data collection • Potential negative implications • Location tracking • Lack of awareness • Transparency • Data control • Attribution of trust • Sharing criteria	• Pay for privacy enhancing (+) • Usability (−)	Islami et al. (2022)
Sweden, UK, Germany, USA, Ireland, Greece, Singapore, China, Netherlands	36 experts in the academia and the industry	Semi-structured interviews	• Awareness • User and vendor education • Safety • Responsibility • Legislation • Trust	NA	Liu et al. (2020)
South Africa	16 road users	Semi-structured interviews	• Awareness • User and vendor education • Safety • Responsibility • Legislation • Trust	• Travel safety (+) • Usability (+) • Pay for privacy enhancing (−)	Islami et al. (2021)

Note: The symbols (+) and (−) indicate whether individuals were in favour or not in favour of balancing specific perceived benefits against privacy concerns. They do not reflect any quantitative measurement of significance.

reflected their genuine reactions and concerns from data collection across different emerging technologies.

Thematic analysis of the workshop data revealed six main themes of concern: (1) privacy, (2) technology, (3) data security, (4) awareness of data collection, (5) consequences of data collection, and (6) the involvement of third parties. The analysis also highlighted strong interconnections across those concerns. For example, worries about third parties emerged when road users were unclear about data-sharing arrangements and the purposes for which data would be used. Similarly, concerns about the potential negative consequences of data collection were linked to uncertainties around data-sharing practices. Participants expressed a desire for greater control over who the third parties and data storage providers would be, underscoring their need to maintain control over their personal data. Additionally, concerns related to technology included requests for more detailed information about the types of data collected through new technologies.

Compared to previous privacy literature, this study identified additional dimensions of concern beyond privacy issues. Specifically, the privacy concerns observed in this study included: (1) the types of data collected, (2) data sharing recipients, (3) control over personal data, (4) risks of data misuse, (5) data retention duration, and (6) platforms for data sharing when adopting new technologies; these findings were consistent with previous studies (McCarthy et al. 2016; Patil et al. 2016b; van den Boogert & Ding 2023). Beyond these privacy aspects, this study uncovered further areas of concern, including technology-related issues, data security, awareness of data collection, potential consequences arising from data use, and the involvement of third parties.

As shown in Table 4, findings in this study align with those by Liu et al. (2020), who reported insights from expert interviews on cybersecurity and privacy challenges related to the acceptance of CAVs. The interconnected themes identified in their study included awareness, user and vendor education, responsibility, safety, legislation, and trust. It is important to note that Liu et al. (2020) analysed the views of experts in cyber security, privacy and CAVs without necessarily asking them to assume the role of CAV user. This suggests that the themes reflect what experts believe is needed to facilitate road users' acceptance of CAVs. In contrast, this study captures the direct perspectives and specific demands of road users themselves. Consistent with Liu et al. (2020), participants in this study also emphasised the importance of awareness, user education, shared responsibility among multiple stakeholders, and cybersecurity.

Similarly, Islami et al. (2022) reported on participant considerations when adopting intelligent vehicular communication systems (see, Table 4). Their study, which involved semi-structured interviews with road users in Sweden, identified themes including comfort with data collection, concerns over location tracking, potential risks such as hacking, data abuse involving of unwanted third parties, awareness of data collection, transparency, data control, perceived trust in various actors, and conditions for data sharing (e.g., for safety or emergency situations, sharing with family, police and government). Notably, all the themes are reflected in this study underscoring a comprehensive overlap of user concerns across different contexts. However, unlike Islami et al. (2022), this study uniquely emphasises specific concerns related to data security data security – such as data encryption, data breaches, data storage, and cybersecurity threats – as well as the critical importance of fairness and inclusivity in the adoption of new technologies.

The thematic analysis of the workshops further identified two key trade-offs related to data privacy: (1) road safety, and (2) the usability of new technologies such as providing real-time travel information. Similar privacy trade-offs have been reported in previous studies, including monetary costs to enhance data privacy (Islami et al. 2022), financial incentives for exchanging personal data (Hunecke et al. 2021; Boogert & Ding 2023), technology usability (Rodríguez-Priego et al. 2022), safety benefits provided by the technology (McCarthy et al. 2016; Patil et al. 2016b; Picco et al. 2023), and environmental benefits associated with technology adoption (Rahimi et al. 2020; Chen et al. 2023).

Cultural differences appear to significantly influence the types of trade-offs road users are willing to make (Pati et al. 2016a; Potoglou et al. 2017). For example, as shown in Table 4, Islami et al. (2022) found that Swedish drivers placed greater value on Privacy Enhancing Technologies (PETs), with the majority willing to pay for pseudonymization services. They were also reluctant to sacrifice privacy by sharing location data for usability benefits such as finding open parking spaces. In contrast, South African drivers demonstrated less willingness to pay for PETs and were more open to sharing location information when it enhanced safety (Islami et al. 2021). These differences in trade-off likely reflect varying cultural attitudes towards privacy, feelings of security, and trust in government data protection (Patil et al. 2016a; Islami et al. 2022).

Addressing road users' privacy concerns is crucial for the wider acceptance and adoption of new technologies within the 'Digital Roads' initiative. Developing an ethical framework that defines key principles is crucial to support this technological transition, ensuring enhanced safety and the provision of vital information to road users (Bonnefon et al. 2020). This study contributes valuable insights and initiates an important dialogue on the practical and ethical implications of emerging digital road technologies.

The ethical principles for responsible innovation (Pandza and Ellwood 2013)– such as transparency, awareness, data security, fairness, inclusiveness, and accountability – should form the six key areas of focus for the transport sector in addressing road users' privacy concerns related to data collection when implementing new technologies. Transparency (Patil et al. 2016b; Segkouli et al. 2022) and awareness (Liu et al. 2020) are fundamental principles that require clear and open communication with road users regarding how their data is used. This entails providing detailed information about data usage, data-sharing practices, the technologies involved, and the potential consequences of data misuse. To foster trust and confidence, awareness-raising about data collection on digital roads should be supported by comprehensive educational campaigns delivered both online (e.g., social networks) and offline (e.g., strategically placed information at key locations).

Data security is another important ethical principle that extends beyond the responsibilities of the data collectors and data managers to include all stakeholders in data collection processes (Acharya and Mekker 2022). To safeguard the integrity and confidentiality of collected data and minimise cybersecurity risks, robust measures such as encryption protocols (Aliebrahimi and Miller 2023), data anonymisation (Patil et al. 2016a), strict access controls (Babun et al. 2021), and regular security audits (Uddin et al. 2021), must be rigorously implemented. Additionally, the ethical principles of fairness and inclusiveness highlight the importance of

equitable access to technologies and services for all road users (Segkouli et al. 2022). Efforts to reduce bias in AI-driven solutions and promote fairness in service delivery are critical to fostering a more inclusive transportation ecosystem.

In multi-stakeholder environments, it is critical to establish clear accountability frameworks (Patil et al. 2016b). Such frameworks not only ensure that each stakeholder understands their role and obligations thus reducing confusion and potential conflicts, but also build trust among stakeholders, including users and regulatory bodies, thereby creating a positive environment for the adoption of new technologies.

6. Conclusion

The road transport sector is rapidly embracing road digitalisation initiatives, such as "Digital Roads," which utilise advanced technologies such as AI and CAV systems to enhance user experience, safety, and network efficiency. This transformation, however, requires robust data governance and ethical frameworks that prioritise not only compliance but the secure and responsible handling of user data. These frameworks should cater for the evolving needs road users' within an increasingly connected environment. Although several frameworks currently exist, many are not specifically designed to meet the unique demands of transport and digital road networks. They often overlook the perspectives of road users' and the behavioural factors that are essential to establish a balanced, ethical approach to data use in this sector.

This study lays the foundation and outlines the next steps for designing an ethical framework tailored specifically to road transport and digital innovation within the sector. This study contributes to an emerging body of knowledge concerned with understanding road users' concerns related to data collection amid the adoption of new technologies in the context of digital roads. Road users primarily expressed concerns about data privacy, security, awareness of data collection practices, potential consequences, and third-party involvement. This perspective offers richer, more detailed insights into how individuals perceive and are impacted by privacy issues in the context of the 'Digital Roads' initiative. Such insights are essential for the development of user-centric ethical policies that address specific user needs within the digital transformation of transport.

By adopting this user-centred approach to addressing concerns around new technologies, measures can be developed to mitigate road users' privacy concerns. For example, creating accessible feedback platforms (e.g., apps or online surveys) would enable organisations to respond to real-time concerns, promote transparency, and support responsible innovation. Also, ensuring and communicating the safety and user benefits of new technologies can further increase road user acceptance, creating a more favourable environment for digital advancements in transport.

By embedding six ethical principles – transparency, awareness, data security, fairness, inclusiveness, and accountability – to address road users' primary concerns around data collection using new technologies, road transport organisations can develop ethical frameworks to protect users' data rights and strengthen public trust in digital road transformation. Also, scientific governance strategies that promote data ethics and protect road users' data privacy are essential within these organisations. Such strategies could involve regularly gathering feedback from road users and stakeholders, establishing dedicated professional groups focused on data ethics, and engaging in collaborative efforts to promote responsible data practices.

These guidelines further suggest actionable dimensions for the development of an ethical framework that may be applicable to road organisations and other public service providers centred around three core responsibilities: (a) do good (e.g, building road users' awareness and fostering understanding of data practices), (b) no harm (e.g., ensuring transparency, data security, fairness, and inclusivity), and (c) responsible governance (e.g., accountability and ethical oversight). More broadly, this study contributes to the critical area of public policy by highlighting the importance of social research in shaping organisational strategies across industries beyond transport, such as ethical decision-making and data management practices within public and private operators or organisations.

Future research should aim to involve a broader and more diverse sample base of road users. For example, a limitation of this study is that most participants were primarily from academia and some specialised in Computer Science. The qualitative interviews did reach saturation, and this group of participants helped to provide an in-depth, specialist insight of the challenges regarding the implications of 'Digital Roads'. Evidence from a wider array, non-specialist road users, however, would help mitigate potential biases and enrich understanding of public concerns.

Building robust evidence of the nuanced privacy issues pertaining 'Digital Roads' and their implications through qualitative analyses, such as this study, can inform the development of targeted survey campaigns that ensure representative data and generalisable findings for the broader road user population. Given that discourses around privacy and digital roads are dynamic and evolving, it is necessary to conduct comparative studies across different countries and contexts to better understand how privacy concerns vary globally. Future research could also focus on investigating user trade-offs between privacy protection and potential benefits, through studies and experiments, to build a strong evidence base that supports informed decision-making and the development of user-centred data frameworks for digital roads.

CRediT authorship contribution statement

Rongqiu Song: Writing – review & editing, Writing – original draft, Visualization, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Dimitris Potoglou:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Investigation, Conceptualization. **Nadeem Fayyaz:** Writing – review & editing, Resources, Methodology, Investigation, Data curation, Conceptualization. **Mehreen Ashraf:** Writing – review & editing, Methodology, Conceptualization. **Katarzyna Stawarz:** Writing – review & editing, Conceptualization. **George Theodorakopoulos:** Writing – review & editing, Conceptualization.

Tim Edwards: Writing – review & editing, Conceptualization. **Emyr Thomas:** Writing – review & editing, Resources, Methodology, Conceptualization. **Yulia Cherdantseva:** Writing – review & editing, Supervision, Resources, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization.

Funding

This study was funded as part of the 'Cyber Futures' project on behalf of National Highways, UK.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors wish to thank Omkar D. Deshmukh for his assistance in the early stages of the project. The authors also wish to acknowledge the support of the Digital Transformation Innovation Institute at Cardiff University in facilitating this project; with special thanks to Julie Hayward for project coordination.

Appendix A. . Workshop materials

.

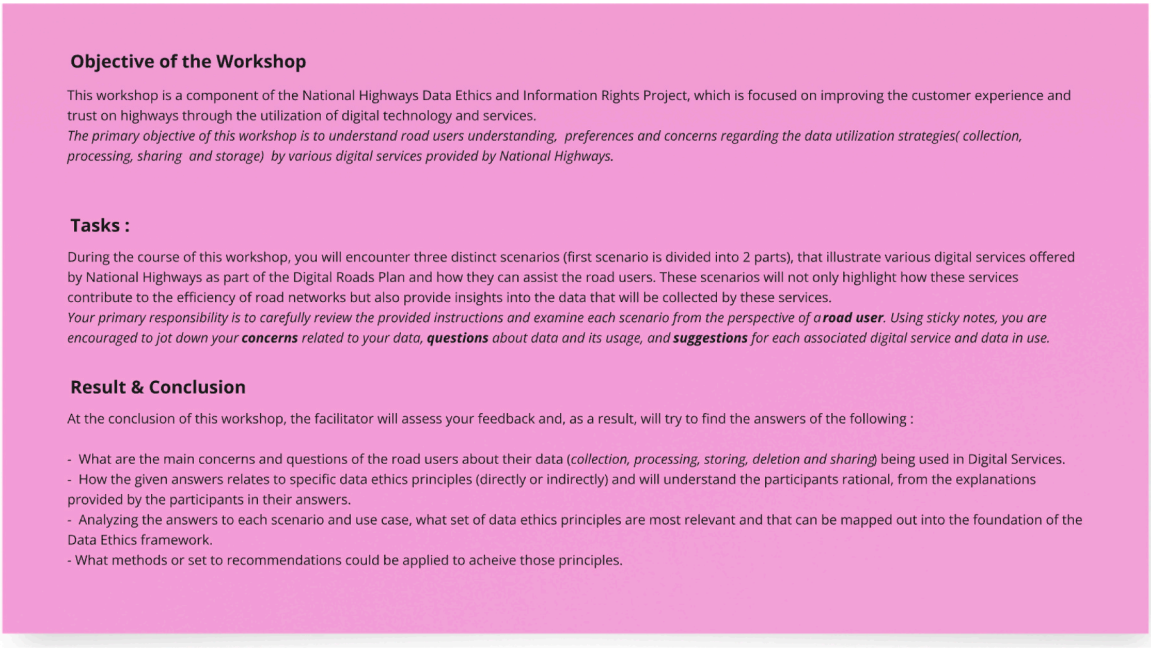

Fig. A1. Introduction to the workshop

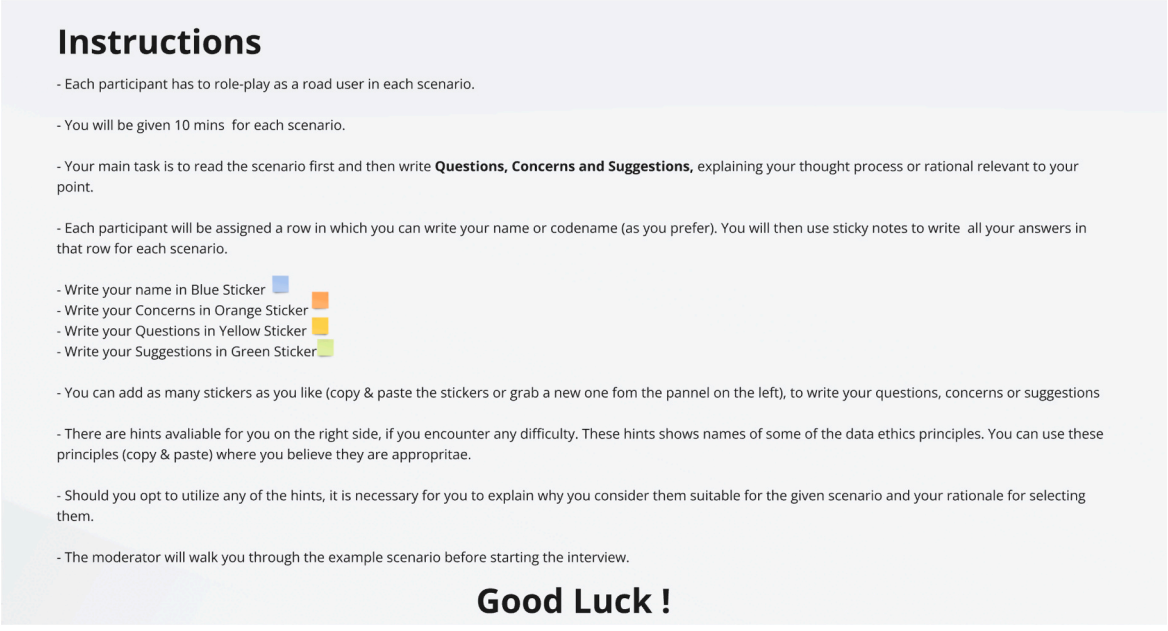

Fig. A2. Workshop instructions

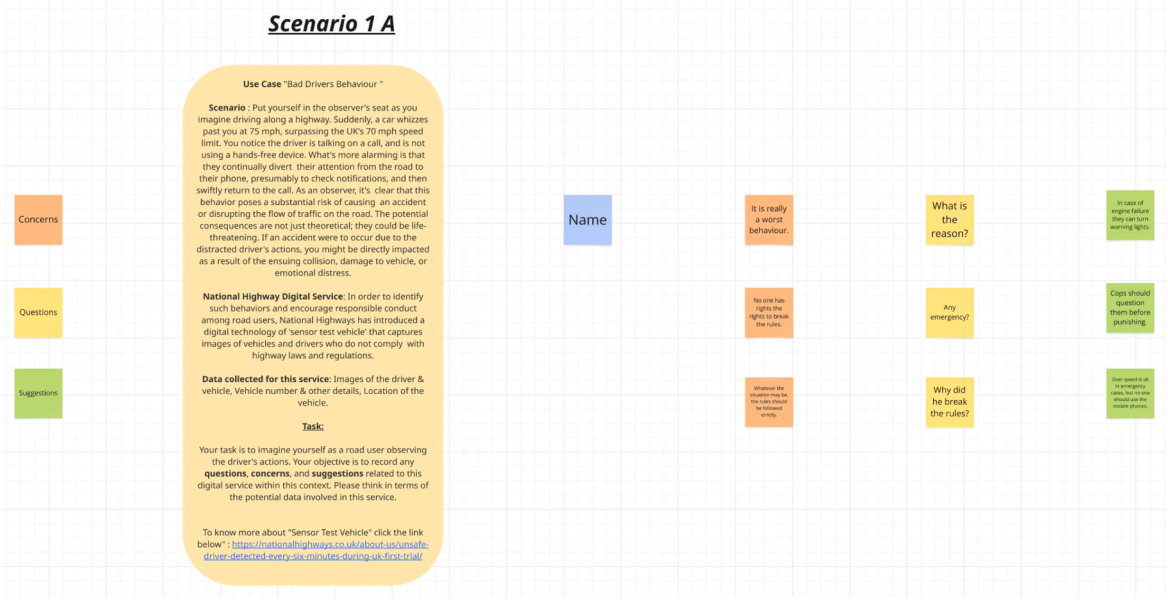

Fig. A3. An example of a response to a workshop scenario on Miro

Data availability

The authors do not have permission to share data.

References

Acharya, S. and Mekker, M. 2022. Importance of the reputation of data manager in the acceptance of connected vehicles. *Communications in Transportation Research* 2 (December 2021), p. 100053. Available at: doi: 10.1016/j.commtr.2022.100053.

Acheampong, R.A., Legacy, C., Kingston, R. and Stone, J. 2023. Imagining urban mobility futures in the era of autonomous vehicles—insights from participatory visioning and multi-criteria appraisal in the UK and Australia. *Transport Policy* 136, pp. 193–208. Available at: doi: 10.1016/j.tranpol.2023.03.020.

Adams, W.C. 2015. Conducting Semi-Structured Interviews. In: *Handbook of Practical Program Evaluation: Fourth Edition*. doi: 10.1002/9781119171386.ch19.

Aliebrahimi, S. and Miller, E.E. 2023. Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour* 96(May 2022), pp. 82–91. Available at: doi: 10.1016/j.trf.2023.06.010.

Babun, L., Denney, K., Celik, Z.B., McDaniel, P. and Uluagac, A.S. 2021. A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks* 192(January), p. 108040. Available at: doi: 10.1016/j.comnet.2021.108040.

Bonnefon, J.-F., et al. (2020). *Ethics of Connected and Automated Vehicles: Recommendations on road safety, privacy, fairness, explainability, and responsibility*. *Available at*. https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en.

van den Boogert, R. J., & Ding, A. Y. (2023). Engaging the crowd in sensing for smart mobility: A discrete choice experiment. *IEEE Open Journal of Intelligent Transportation Systems, 4*, 406–418. https://doi.org/10.1109/OJITS.2023.3277311

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Chen, Y., Khalid Khan, S., Shiwakoti, N., Stasinopoulos, P. and Aghabayk, K. 2023. Analysis of Australian public acceptance of fully automated vehicles by extending technology acceptance model. *Case Studies on Transport Policy* 14(February), p. 101072. Available at: doi: 10.1016/j.cstp.2023.101072.

Cottrill, C.D. and Vonu Thakuriah, P. 2015. Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C: Emerging Technologies* 56, pp. 132–148. Available at: doi: 10.1016/j.trc.2015.04.005.

Creswell, J.W. 1998. Qualitative inquiry and research design: Choosing among five traditions.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*. https://doi.org/10.1287/orsc.10.1.104

Englund, C., Aksoy, E. E., Alonso-Fernandez, F., Cooney, M. D., Pashami, S., & Åstrand, B. (2021). Ai perspectives in smart cities and communities to enable road vehicle automation and smart traffic control. *Smart Cities, 4*(2), 783–802. https://doi.org/10.3390/smartcities4020040

Parliament, E. (2016). *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An Experiment with Data Saturation and Variability. *Field Methods, 18*(1). https://doi.org/10.1177/1525822X05279903

Hunecke, M., Richter, N. and Heppner, H. 2021. Autonomy loss, privacy invasion and data misuse as psychological barriers to peer-to-peer collaborative car use. *Transportation Research Interdisciplinary Perspectives* 10, p. 100403. Available at: doi: 10.1016/j.trip.2021.100403.

Islami, L., Fischer-Hübner, S., Hammond, E. N. K., & Eloff, J. (2021). Analysing Drivers' Preferences for Privacy Enhancing Car-to-Car Communication Systems: A Study from South-Africa. In *In: IFIP Advances in Information and Communication Technology*. https://doi.org/10.1007/978-3-030-72465-8_7

Islami, L., Fischer-Hübner, S. and Papadimitratos, P. 2022. Capturing drivers' privacy preferences for intelligent transportation systems: An intercultural perspective. *Computers and Security* 123, p. 102913. Available at: doi: 10.1016/j.cose.2022.102913.

Kleizen, B., Van Dooren, W., Verhoest, K. and Tan, E. 2023. Do citizens trust trustworthy artificial intelligence? Experimental evidence on the limits of ethical AI measures in government. *Government Information Quarterly* (March), p. 101834. Available at: doi: 10.1016/j.giq.2023.101834.

Liu, N., Nikitas, A. and Parkinson, S. 2020. Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology and Behaviour* 75, pp. 66–86. Available at: doi: 10.1016/j.trf.2020.09.019.

Ljubi, K., & Groznik, A. (2023). Role played by social factors and privacy concerns in autonomous vehicle adoption. *Transport Policy, 132*, 1–15. https://doi.org/10.1016/j.tranpol.2022.12.013

Maguire, M., & Delahunt, B. (2017). *Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars. All Ireland Journal of Teaching and Learning in Higher Education n, AISHE-J) (3*, 3351–33514.

McCarthy, O. T., Caulfield, B., & O'Mahony, M. (2016). How transport users perceive personal safety apps. *Transportation Research Part F: Traffic Psychology and Behaviour, 43*, 166–182. https://doi.org/10.1016/j.trf.2016.10.005

Highways, N. (2021). *Introduction to Digital roads*. Available at: https://nationalhighways.co.uk/media/2chotw13/introducing-digital-roads.pdf.

National Highways. 2022. *New research van rolled out to detect dangerous driving*. Available at: https://nationalhighways.co.uk/our-work/innovation-and-research/news/new-research-van-rolled-out-to-detect-dangerous-driving/#:~:text=The "sensor test vehicle" is,were without a seat belt.

National Highways. 2023. *Digital Roads*. Available at: https://nationalhighways.co.uk/our-work/digital-data-and-technology/digital-roads/.

National Highways. 2024a. *Digital Roads*. Available at: https://nationalhighways.co.uk/our-work/digital-data-and-technology/digital-roads/ [Accessed: 29 August 2024].

National Highways. 2024b. *Stopped vehicle detection upgrades*. Available at: https://nationalhighways.co.uk/our-work/smart-motorways-evidence-stocktake/stopped-vehicle-detection-upgrades/#:~:text=Stopped vehicle detection enables us,limits and deploying traffic officers.

Olovsson, T., Svensson, T. and Wu, J. 2022. Future connected vehicles: Communications demands, privacy and cyber-security. *Communications in Transportation Research* 2, p. 100056 Contents. doi: 10.1016/j.commtr.2022.100056.

Paiva, S., Ahad, M.A., Zafar, S., Tripathi, G., Khalique, A. and Hussain, I. 2020. Privacy and security challenges in smart and sustainable mobility. *SN Applied Sciences* 2(7), pp. 1–10. Available at: doi: 10.1007/s42452-020-2984-9.

Pandza, K. and Ellwood, P. 2013. Strategic and ethical foundations for responsible innovation. *Research Policy* 42(5), pp. 1112–1125. Available at: doi: 10.1016/j.respol.2013.02.007.

Patil, S., Patruni, B., Potoglou, D. and Robinson, N. 2016b. Public preference for data privacy – A pan-European study on metro/train surveillance. *Transportation Research Part A: Policy and Practice* 92, pp. 145–161. Available at: doi: 10.1016/j.tra.2016.08.004.

Patil, S., Potoglou, D., Lu, H., Robinson, N. and Burge, P. 2014. Trade-off Across Privacy, Security and Surveillance in the Case of Metro Travel in Europe. *Transportation Research Procedia* 1(1), pp. 121–132. Available at: doi: 10.1016/j.trpro.2014.07.013.

Picco, A., Stuiver, A., de Winter, J. and de Waard, D. 2023. The use of monitoring and feedback devices in driving: An assessment of acceptability and its key determinants. *Transportation Research Part F: Traffic Psychology and Behaviour* 92(October 2022), pp. 1–14. doi: 10.1016/j.trf.2022.10.021.

Potoglou, D., Dunkerley, F., Patil, S. and Robinson, N. 2017. Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior* 75, pp. 811–825. Available at: doi: 10.1016/j.chb.2017.06.007.

Potoglou, D., Palacios, J.F. and Feijóo, C. 2015. An integrated latent variable and choice model to explore the role of privacy concern on stated behavioural intentions in e-commerce. *Journal of Choice Modelling* 17, pp. 10–27. Available at: doi: 10.1016/j.jocm.2015.12.002.

Potoglou, D., Whittle, C., Tsouros, I. and Whitmarsh, L. 2020. Consumer intentions for alternative fuelled and autonomous vehicles: A segmentation analysis across six countries. *Transportation Research Part D: Transport and Environment* 79(January), p. 102243. Available at: doi: 10.1016/j.trd.2020.102243.

Rahimi, A., Azimi, G., Asgari, H. and Jin, X. 2020. Adoption and willingness to pay for autonomous vehicles: Attitudes and latent classes. *Transportation Research Part D: Transport and Environment* 89(November), p. 102611. Available at: doi: 10.1016/j.trd.2020.102611.

Rodríguez-Priego, N., Porcu, L. and Kitchen, P.J. 2022. Sharing but caring: Location based mobile applications (LBMA) and privacy protection motivation. *Journal of Business Research* 140, pp. 546–555. Available at: doi: 10.1016/j.jbusres.2021.11.022.

Rodwell, D., Ho, B., Pascale, M.T., Elrose, F., Neary, A. and Lewis, I. 2023. In their own words : A qualitative study of users ' acceptance of connected vehicle technology after nine months of experience with the technology. *Transportation Research Part F: Psychology and Behaviour* 97, pp. 73–93. Available at: doi: 10.1016/j.trf.2023.07.004.

Patil, S., Lu, H., Saunders, C. L., Potoglou, D., & Robinson, N. (2016a). Public preferences for electronic health data storage, access, and sharing - evidence from a pan-European survey. *Journal of the American Medical Informatics Association, 23*(6), 1096–1106. https://doi.org/10.1093/jamia/ocw012

Segkouli, S., et al. (2022). Ethical Decision making in Iot Data Driven Research: A Case Study of a Large-Scale pilot. *Healthcare (Switzerland), 10*(5). https://doi.org/10.3390/HEALTHCARE10050957

Singh, R., Sharma, R., Vaseem Akram, S., Gehlot, A., Buddhi, D., Malik, P.K. and Arya, R. 2021. Highway 4.0: Digitalization of highways for vulnerable road safety development with intelligent IoT sensors and machine learning. *Safety Science* 143(July), p. 105407. Available at: doi: 10.1016/j.ssci.2021.105407.

Song, R. and Potoglou, D. 2024. Electric vehicle public charging choices: a qualitative investigation. *Transportation Planning and Technology*, pp. 1–23. Available at: doi: 10.1080/03081060.2024.2367754.

Swedish Transport Administration. (2022). *Roadmap – Digitalisation of the Road Transport System*. Available at: https://www.connectedautomateddriving.eu/wp-content/uploads/2023/06/FULLTEXT01-1.pdf.

U.S. Department of Transportation Federal Highway Administration. 2020. *Collaborating for the Future of Transportation*. Available at: https://highways.dot.gov/public-roads/winter-2020/collaborating-future-transportation.

Uddin, M.A., Stranieri, A., Gondal, I. and Balasubramanian, V. 2021. A survey on the adoption of blockchain in IoT: challenges and solutions. *Blockchain: Research and Applications* 2(2), p. 100006. Available at: doi: 10.1016/j.bcra.2021.100006.

Walter, J. and Abendroth, B. 2020. On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services. *Telematics and Informatics* 49, p. 101361. Available at: doi: 10.1016/j.tele.2020.101361.

Yao, H. et al. 2023. Advanced industrial informatics towards smart, safe and sustainable roads: A state of the art. *Journal of Traffic and Transportation Engineering (English Edition)* 10(2), pp. 143–158. Available at: doi: 10.1016/j.jtte.2023.02.001.

Ying, S., Huang, Y., Qian, L. and Song, J. 2023. Privacy paradox for location tracking in mobile social networking apps: The perspectives of behavioral reasoning and regulatory focus. *Technological Forecasting and Social Change* 190(February), p. 122412. Available at: doi: 10.1016/j.techfore.2023.122412.