Transportation Research Part F 75 (2020) 66–86

Contents lists available at ScienceDirect

Transportation Research Part F

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

# Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach

Na Liu, Alexandros Nikitas *, Simon Parkinson

*University of Huddersfield, Huddersfield, UK*

ARTICLE INFO

*Article history:*
Received 7 March 2020
Received in revised form 11 August 2020
Accepted 22 September 2020
Available online 22 October 2020

*Keywords:*
Connected and autonomous vehicles
Cyber security
Privacy
User acceptance
Thematic analysis

ABSTRACT

Connected and Autonomous Vehicles (CAVs) constitute an automotive development carrying paradigm-shifting potential that may soon be embedded into a dynamically changing urban mobility landscape. The complex machine-led dynamics of CAVs make them more prone to data exploitation and vulnerable to cyber attacks than any of their predecessors increasing the risks of privacy breaches and cyber security violations for their users. This can adversely affect the public acceptability of CAVs, give them a bad reputation at this embryonic stage of their development, create barriers to their adoption and increased use, and complicate the business models of their future operations. Therefore, it is vital to identify and create an in-depth understanding of the cyber security and privacy issues associated with CAVs, and of the way these can be prioritised and addressed. This work employs 36 semi-structured elite interviews to explore the diverse dimensions of user acceptance through the lens of the well-informed CAV experts that already anticipate problems and look for their solutions. Our international interviewee sample represents academia, industry and policy-making so that all the key stakeholder voices are heard. Thematic analysis was used to identify and contextualise the factors that reflect and affect CAV acceptance in relation to the privacy and cyber security agendas. Six core themes emerged: *awareness, user and vendor education, safety, responsibility, legislation, and trust*. Each of these themes has diverse and distinctive dimensions and are discussed as sub-themes. We recommend that mitigating the cyber security and privacy risks embedded in CAVs require inter-institutional cooperation, awareness campaigns and trials for trust-building purposes, mandatory educational training for manufacturers and perhaps more importantly for end-users, balanced and fair responsibility-sharing, two-way dynamic communication channels and a clear consensus on what constitutes threats and solutions.


## 1. Introduction

Connected and Autonomous Vehicles (CAVs) are a technology, still in its infancy, with the potential, if used responsibly, to transform automotive transport and urban landscapes (Nikitas, Njoya, & Dani, 2019). CAVs have been introduced as a subset of the Cyber-Physical Systems (CPSs), in the context of highway transportation, which consists of digital software platforms, physical infrastructure and human components. The advent of CAVs has gained worldwide attention and traction, promising

* Corresponding author.
*E-mail address:* a.nikitas@hud.ac.uk (A. Nikitas).

https://doi.org/10.1016/j.trf.2020.09.019
1369-8478/

**Nomenclature**

*List of Acronyms*

| | |
|---|---|
| **CAVs** | Connected and Autonomous Vehicles |
| **RDSP** | Federal Cyber security Research and Development Strategic Plan |
| **NPRS** | National Privacy Research Strategy |
| **NSTC** | National Science and Technology Council |
| **CPSs** | Cyber-Physical systems |
| **SAE** | Society of Automotive Engineers |
| **AV** | Autonomous Vehicle |
| **CV** | Connected Vehicle |
| **V2V** | Vehicle-to-Vehicle |
| **V2I** | Vehicle-to-Infrastructure |
| **V2X** | Vehicle-to-Everything |
| **V2N** | Vehicle-to-Network |
| **OICA** | International Organisation of Motor Vehicle Manufacturers |
| **ITS** | Intelligent Transportation System |
| **CAR** | Center for Automotive Research |
| **WTP** | Willingness to Pay |
| **MLP** | Multi-Level Perspective |
| **TAM** | Technology Acceptance Model |
| **NTD** | National Transit Database |
| **ISPs** | Internet Service Providers |
| **OOH** | Outdoor or Out of Home |
| **HMI** | Human-Machine Interface |

economic, social and environmental benefits that can establish the era of the smart city. More specifically: from an economic perspective, CAVs can facilitate the reduction of energy costs (Rios-Torres & Malikopoulos, 2016), improve fuel economy (Vahidi & Sciarretta, 2018), create more productive time (Clements & Kockelman, 2017), promote inclusive economic growth (Meyer, Becker, Bösch, & Axhausen, 2017); from a social perspective, CAVs are marketed for their increased accident prevention and traffic safety merits (Ye & Yamamoto, 2019), potential to alleviate traffic congestion (Talebpour & Mahmassani, 2016), beneficial impact on public health and wellbeing (Faisal, Yigitcanlar, Kamruzzaman, & Currie, 2019), improvement of travel behaviour (Taiebat, Stolper, & Xu, 2019), increased travel equality and accessibility (Goggin, 2019); from an environmental perspective, CAVs can help in reducing emissions and air pollution (Bauer, Greenblatt, & Gerke, 2018), lessening energy consumption (Wadud, MacKenzie, & Leiby, 2016), optimising fuel use (Mamouei, Kaparias, & Halikias, 2018), preventing environmental degradation (Bagloee, Tavana, Asadi, & Oliver, 2016) and decreasing noise nuisance (Nikitas, Kougias, Alyavina, & Njoya Tchouamou, 2017). The UK government, for example, is encouraging CAV technology development through the current National Infrastructure Delivery Plan (2016–2021).

At the same time and despite the huge potential of CAVs to deliver the listed improvements, these new vehicles are also linked to some significant concerns referring to traffic safety and moral issues (Liljamo, Liimatainen, & Pöllänen, 2018); effective interaction between CAVs and other forms of travel including pedestrians (Palmeiro et al., 2018); excessive traffic and unoccupied vehicle trips (Cohen & Hopkins, 2019); displacement of driving professionals (Heard, Taiebat, Xu, & Miller, 2018); lack of situational awareness and difficult behavioural adaption for the users (Strand, Nilsson, Karlsson, & Nilsson, 2014); and drivers' unwillingness to forfeit driving (Tennant, Stares, & Howard, 2019), among others. Cyber security and privacy risks have also emerged as a key challenge because of CAVs susceptibility to hacking and data exploitation (Nikitas et al., 2019). As with all connected computing infrastructures, increasing the level of computational functionality and connectivity in vehicles increases their exposure to potential vulnerabilities (Parkinson, Ward, Wilson, & Miller, 2017), as well as creating new opportunities for data mismanagement. Security and privacy are critical concerns that may hinder the wide deployment of CPSs if not properly addressed (Giraldo, Sarkar, Cardenas, Maniatakos, & Kantarcioglu, 2017). The connected physical world suffers not only from the attacks targeting today's networked systems, but also from new ones that we may not be able to accurately predict today (Sadeghi, Wachsmann, & Waidner, 2015). The fine-grained, heterogeneous, and sensed big data are vulnerable to various inference attacks, causing privacy disclosure and data safety violations (Song, Fink, & Jeschke, 2017), while the controlling devices, sensors and signals can be manipulated to launch attacks that can lead to system instability (Bou-Harb et al., 2017). The complex dynamics that can emerge between the physical, the automated

and the connected dimensions of CAVs create new and unique challenges for end-users, public authorities, car manufacturers and service providers. Therefore, efforts meaning to address privacy and cyber security issues are timely and meaningful.

It is strongly believed that public acceptance will be negatively affected if CAV technology risks are not thoroughly studied (Bou-Harb et al., 2017). Given that the introduction and promotion of CAVs are heavily reliant upon the ubiquitous access and participation, understanding and demystifying acceptance towards CAVs and the associated risks with their use is fundamental to help detect the gaps in their cyber security and privacy and develop effective governance.

This work aims to make the first step in understanding the factors reflecting and affecting CAV acceptance in regards to cyber security and privacy issues through the lens of experts that at this early stage of CAV development are the ones with the knowledge and forecasting ability to help us identify and contextualise the diverse and distinctive dimensions and orientations of this still severely understudied agenda. This will allow us to set out priority areas within this diverse agenda that we could then investigate with the general public. More specifically, we conducted this research by means of elite in-depth interviews with field experts. We seek to uncover their views on some of the emerging trends that will shape the CAV privacy and cyber security policy agenda and how industry, government and universities could work together to help harness the identified opportunities.

The next section provides an overview of the relevant literature on CAVs, cyber security and privacy as well as public attitudes and CAV adoption. The third section describes in detail the methodological approach employed by this study, followed by a section presenting the results of our thematic analysis. Section 5 provides discussion and policy recommendations. Section 6 acknowledges our study's limitations and sketches our future research, while the final section concludes the study by emphasising its importance.

## 2. Background

### *2.1. Defining the terminology of CVs, AVs and CAVs*

For clarity and consistency reasons, it is important to highlight that this work focuses on CAVs. The future of vehicle automation has many different angles and there is a tendency to employ terms like connected car, smart car, autonomous car, driverless car, self-driving car interchangeably. However, a CAV is not synonymous to a Connected Vehicle (CV) or an Autonomous Vehicle (AV); these are different (Talebpour & Mahmassani, 2016).

CV is a vehicle that can communicate and exchange information wirelessly with other vehicles, external networks and infrastructure via Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to-Everything (V2X) technologies, but that does not necessarily mean that CVs are capable of autonomous driving. Fundamentally, the CV end-users would enjoy a set of services integrating information, infrastructure and communication technologies that improve transportation efficiency and security.

AVs are vehicles that are capable of driving themselves without human intervention. This study adopts the International Organization of Motor Vehicle Manufacturers (OICA)'s definition of levels of automation, which is based on the Society of Automotive Engineers (SAE) International Standard J3016 and refers to six levels of autonomy: 0 being no autonomy; 1 being driver assistance; 2 being partial automation; 3 being conditional automation; 4 being high automation; and 5 being full automation. AVs may not be connected although the two technologies can be complementary.

If a vehicle is both connected and autonomous, then it can be classified as a CAV. According to Nikitas, Michalakopoulou, Njoya, and Karampatzakis (2020) CAV is any vehicle able to understand its surroundings, move, navigate and behave responsibly without human input which at the same time has connectivity functions enabling it to be proactive, cooperative, well-informed and coordinated. Our study is specifically discussing expert attitudes about the privacy and cyber security issues of fully enabled CAVs.

### *2.2. Cyber security and privacy*

There are many overlapping terms for cyber security concepts in CAVs including information security, information assurance and network security. For the purposes of this study cyber security is defined, according to the General Data Protection Regulation (GDPR) guidance as 'the use of appropriate technical and organisational measures to secure infrastructure, networks and data from unauthorised or malicious activity'. Cyber security in CAVs according to Olufowobi and Bloom (2019) is the answer to attacks associated with: desire for infamy, vengeance, or twisted pleasure; profit; traffic control so as to create open or congested routes; traffic disruption to create congestion or even panic; intelligence, surveillance, and reconnaissance, whether targeted or en masse; vehicle theft; remote hijacking of an operating vehicle; infecting vehicles with malware; and creating a vehicular botnet. Privacy is 'the act of empowering users to make their own decisions about who can access and process their data and personal space and for what purpose'. Security and privacy are the most critical concerns that may hinder the wide deployment of CPSs in general and CAVs in particular (Song et al., 2017). Possible cyber attacks, maliciously controlled vehicles and software vulnerabilities might compromise the safety levels of CAVs (Milakis, Van Arem, & Van Wee, 2017), while privacy as the ability to move about in relative anonymity will be lost with control over private information and misuse of that private information arising as a key drawback of this vehicle technology (Collingwood, 2017).

CPS technologies blur the lines between the physical and cyber world and between infrastructural and personal spaces creating opportunities for innovation (Karnouskos & Kerschbaum, 2017). This blurring is being engineered into the Internet of Things (IoT) where personal CPSs (such as smartphones and automobiles) bearing personal data can reach up into public infrastructures to access services. Infrastructural technologies such as smart roads, e-government, and city services have become personal by providing private portals into public services (Song et al., 2017). Nevertheless, to the larger CPS community, building economically successful CPSs seems to be the priority, since traditionally security and privacy issues can be resolved via patching. This obviously is inappropriate as security and privacy protection must be considered from the early stages when building a CPS – an important lesson learnt from the evolution of the Internet (Romanou, 2018). To educate today's CPS engineers as well as the next-generation of CPS stakeholders, studies identifying the state-of-the-art techniques and potential challenges in security and privacy of CPS are in need (Aceto, Persico, & Pescapé, 2019). In the public space where CAVs operate, there is little expectation of privacy and choice may not be available (Rosner & Kenneally, 2018). To improve the acceptance of CAVs and facilitate the development of the technological and policy mechanisms to protect privacy, public requirements and concerns must first be investigated (Tanczer, Brass, Elsden, Carr, & Blackstock, 2019).

Security and privacy have in common the concepts of appropriate use and protection of information (Acquisti, 2004). Privacy is often seen as freedom from observation, interference or unnecessary public attention. It is often seen as part of security and is the reason for providing confidentiality and when possible anonymity. On the other hand, privacy has a more dynamic dimension, allowing owners to control their own information. Strikingly, security on some occasions may be considered a violation of privacy (Song et al., 2017). Cohen, Jones, and Cavoli (2017) identified that the cyber security and privacy research field is full of unique challenges stemming from various application domains such as healthcare, smart grids, and smart homes, making non-existent the "one-size-fits-all" type of solutions, and that the integration of "cyber" and "physical" worlds opens the doors for insidious and smart attackers to manipulate the system. This leads to new cyber attacks and defence technologies other than those originated from the traditional computer and network systems. Human-factor researchers and psychologists might improve CAV cyber security and privacy provision by understanding human failure that makes attacks successful, by identifying ways to educate people about safe practices and by proposing ways that could reduce human-induced errors (Linkov, Zámečník, Havlíčková, & Pai, 2019).

### 2.3. Public attitude

Social science research shows that public attitudes and behaviours toward new technology and its associated risks are multiple and diverse and are affected by psychological (Frewer, Howard, & Shepherd, 1998), cultural (Williams, 2004), and cognitive factors (AU & Enderwick, 2000). In turn, underlying beliefs and perceptions about CAVs (Bonnefon, Shariff, & Rahwan, 2016; Howard & Dai, 2014), cyber security threats (Bada, Sasse, & Nurse, 2019; Olmstead & Smith, 2017) and privacy risks (Kokolakis, 2017) have been associated with individual or group demographics. Given these complex dynamics, it is difficult to predict public response to future CAV adoption. However, social scientists have confirmed a few core principles and cognitive structures that frame subsequent attitudes and aid to explain behaviour toward CAVs (e.g. value systems and risk perceptions as per Fraedrich & Lenz, 2016). Cohen et al. (2017) explained the multiple links between socio-psychological factors and the key pathways for designing impactful policy; for example, attitudes informing government action, thereby influencing technological development and hence uptake, and thus leading back to attitudes possibly changing them. Frequently used theoretical models in CAV human factor research refer among others to the Technology Acceptance Model (TAM) (Davis, 1989), Multi-Level Perspective (MLP), or the unified theory of acceptance and use of technology (Venkatesh, Morris, Davis, & Davis, 2003).

### 2.4. Previous research on the topic

The existing literature on CAVs is primarily focused on technical, computer and engineering issues; there is a significantly smaller body of work referring to the nexus of acceptance and policy per se. The human factors research for CAVs is mainly focused on their development phases (Anderson et al., 2014), implementation including policy and practice challenges and user characteristics (Kyriakidis, Happee, & de Winter, 2015), user opinions on CAVs referring to law and liability, public acceptability, attitudes, awareness, willingness to use, willingness to pay (Lang, Mei-Pochtler, Rüßmann, & Mohr, 2015; Regan, Cunningham, Dixit, Horberry, Bender, Weeratunga, & Hassan, 2017; Daziano et al., 2017), and their fit with other road users like pedestrian and cyclists (Deb et al., 2017, 2018; Edwards et al., 2015). Research to CAVs' network security vulnerabilities and privacy breach risks through the lens of human factors is very limited to date with few exemptions (e.g. Lim & Taeihagh, 2018; Sheehan, Murphy, Mullins, & Ryan, 2019; Taeihagh & Lim, 2019), with no study ever looking into collecting and analysing qualitative data reflecting the views of CAV experts about this particular agenda. However since CAVs are widely considered to be the next game-changing mobility technology (Nikitas et al., 2017), their associated vulnerabilities should be proactively identified and mitigation techniques should be subsequently developed for assuring that this complex technology will be soon suitable for use (Parkinson et al., 2017).

### 2.5. Research gaps

The study of perceptions reflecting and affecting acceptance towards CAVs, contain various dimensions including public acceptability, attitudes, awareness, willingness to use and willingness to pay. Several studies in the existing literature surveyed general public acceptance of varying vehicle automation levels. Abraham et al. (2017) found that younger adults were more comfortable with self-driving vehicles than older adults. People with higher trust in and higher awareness of CAV technology reported higher possibilities to accept CAVs (Kaur & Rampersad, 2018; Waytz, Heafner, & Epley, 2014), whereas technology anxiety (Hohenberger, Spörrle, & Welpe, 2016) was found to be one of the strong predictors of people's intention to use or not CAVs.

Cavoli, Phillips, Cohen, and Jones (2017) identified that safety and cyber security are two of the key factors underpinning the public perceptions of CAVs. However, there is a scarcity of studies using primary data to identify how exactly the twin narrative of privacy and cyber security affects perceptions towards CAVs per se and no study adopting a qualitative approach that examines in-depth the drivers underpinning the acceptance process.

Almost all of the previous studies on the topic employed a literature review or a quantitative method, in which perceptions, not strictly focusing on privacy and cyber security, have been examined by closed questionnaires (yes/no, Likert scales or ranking exercises) and referred directly to the general public. Studies looking at expert views including transportation professionals, mobility stakeholders, transport academics and employees of the automotive, insurance and consulting industries have been conducted before but on more general topics as reported by Clark, Parkhurst, and Ricci (2016) and Thomopoulos and Nikitas (2019).

## 3. Research methodology

It appears that a limited range of methodologies has been applied to the study of public perceptions to date when it comes to CAV acceptance (Clark et al., 2016). Most studies employ quantitative survey instruments to investigate public perceptions of CAVs. However, given that most respondents are unlikely to have any real experience of AV technology and to have formed opinions on the very specific areas of cyber security and privacy to date, a survey answered by the general public may yield inconclusive results that involve some forms of bias (e.g. optimism bias, desirability bias or lack of awareness bias) and not advance our understanding. Qualitative research is an appropriate tool for gaining an in-depth exploratory understanding that would allow the identification of themes that can be later investigated quantitively but this can be more effective, if as a starting point, is conducted with people that have a more critical understanding of CAVs and are aware of the privacy and cyber security issues referring to them. Thus, a qualitative study with field experts was adopted for the present study.

### 3.1. Elite interview

In-depth interviews with members of the scientific, political, economic, or social elite provide valuable insights that although could be critical to the exploration of a research topic may not be obvious to the general public (Drew, 2014; Jaremba & Mak, 2014; Leblanc & Schwartz, 2007). This is because information on how 'elites' perceive situations and make key decisions provides a unique perspective that often cannot be obtained through other data collection methods (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2014; Zhang et al., 2007). At the same time though we recognise that elite views might not represent the views of the general public per se and might be prone to a different set of biases (e.g. the attitude object, i.e. CAVs, may be too close or personal for them).

In this research, participants were recruited from nine countries in Europe, Asia and North America. The participants were individuals working in CAV relevant disciplines, ranging from computer security to autonomous vehicle production. We acknowledge that participants from the United Kingdom were over-represented due to the close proximity with the research team; however, we believe that this is not a barrier due to the qualitative character of this work and the generic nature of the questions asked. The interviews were conducted face-to-face or via Skype from March to May 2019. Each interview lasted between 30 and 40 min and was semi-structured. For consistency reasons an interview guide set out the generic framework of the interviewing process, but spontaneous add-ons were allowed to enable the collection of more detailed, rich and vivid answers where necessary. The interview guide is presented in the Appendix.

The interview guide had four key dimensions that would allow each participant to:

1. identify the current challenges underpinning the privacy of CAVs;
2. identify the current challenges underpinning the cyber security of CAVs;
3. to make recommendations of cross-domain countermeasures that could be applied to the challenges identified; and
4. to review the areas of responsibility, education and training reflecting and affecting CAV uptake and usage.

**Table 1**
Six-step process for the thematic analysis.

| |
|---|
| Step 1: Familiarising with data |
| Step 2: Generating initial coding |
| Step 3: Searching for themes |
| Step 4: Reviewing of themes |
| Step 5: Defining and naming of themes |
| Step 6: Reporting the findings |

**Table 2**
Interviewee characteristics.

| Respondents | Title | Gender | Country | Position |
|---|---|---|---|---|
| CO1 | Dr | M | Sweden | Senior Researcher |
| CO2 | Dr | M | Sweden | Senior Consultant |
| CO3 | Mr. | M | UK | Research Analyst |
| CO4 | Dr | F | UK | Senior Consultant |
| CO5 | Ms. | F | UK | Principal Consultant |
| OR1 | Dr | M | Germany | Lead Tech |
| OR2 | Dr | M | UK | Chair |
| OR3 | Ms. | F | Germany | Senior Project Manager |
| GO1 | Dr | M | UK | Lead Tech |
| GO2 | Dr | M | UK | Lead Innovation |
| GO3 | Mr. | M | UK | Principal Consultant |
| GO4 | Dr | M | USA | Senior Research Scientist |
| IN1 | Mr. | M | UK | Senior Project Manager |
| IN2 | Prof | M | UK | Head of Department |
| IN3 | Ms. | F | UK | Director |
| IN4 | Mr. | M | USA | CEO & Founder |
| IN5 | Dr | M | Germany | Senior Partner |
| IN6 | Mr. | M | Germany | Senior Project Manager |
| IN7 | Dr | M | Ireland | Associate Director & Lead Tech |
| IN8 | Dr | F | Sweden | Researcher |
| AC1 | Dr | F | UK | Senior Lecturer |
| AC2 | Dr | M | UK | Project Officer |
| AC3 | Dr | M | Greece | Research Associate |
| AC4 | Prof | M | UK | Professor |
| AC5 | Dr | M | USA | Lead Tech |
| AC6 | Dr | M | UK | Research Associate |
| AC7 | Dr | M | UK | Senior Lecturer |
| AC8 | Prof | M | Singapore | Assistant Professor |
| AC9 | Prof | M | UK | Professor |
| AC10 | Dr | M | UK | Senior Lecturer |
| AC11 | Dr | M | UK | Senior Lecturer |
| AC12 | Dr | M | UK | Lecturer |
| AC13 | Prof | M | China | Professor |
| AC14 | Dr | M | UK | Researcher |
| AC15 | Prof | M | UK | Professor |
| AC16 | Dr | F | Netherlands | Lecturer |

### 3.2. Recruitment

Interviewees who occupy management and senior positions in the automotive industry, cyber security firms, universities, government and law consulting firms were targeted to participate in the research. Social media, in particular the LinkedIn platform, were used as a recruitment tool. We recruited field experts by sending interview requests via the LinkedIn message service to the targeted participants (i.e. non-probability convenience sampling). We also used to some degree snowballing sampling, since directly recruited participants recommended some of their colleagues who could be potentially interested to participate in the study. No financial participation incentives were provided for our recruitment purposes. As a whole, 100 experts were targeted and subsequently formally contacted with an online interview invitation; 65 responded back to us, some of them declining the invitation right away others cancelling their participation later on due to availability shortage. At the end 36 interviews were conducted. The participants were informed prior to their involvement about the interview arrangements; it was communicated to and agreed with them that the sessions would be audio recorded and transcribed, but the data would be anonymised and used only for research purposes. Consent for participation and data use was obtained by all the interviewees.

### 3.3. Method of analysis

Thematic analysis was used as detailed in Braun and Clarke (2006) and adapted in Nikitas, Avineri, and Parkhurst (2018) and Nikitas, Wang, and Knamiller (2019) for identifying, analysing and reporting patterns (themes) within data collected in the interviews. Braun and Clarke's (2006) reflexive thematic analysis approach seeks to develop a fluid and recursive frame which is somewhat different from the rigid and structured frame that the traditional codebook approach uses. Table 1 presents the six steps of our thematic analysis process. Thematic analysis has been used before in transport research (Alyavina, Nikitas, & Njoya, 2020; Gössling, Cohen, & Hares, 2016; Hafner, Walker, & Verplanken, 2017) and has proven to be a sophisticated qualitative tool that allows conducting research in a precise, consistent and exhaustive manner through recording,

systematising, and disclosing the methods of analysis and the study results with enough detail to enable the reader to determine the credibility and validity of the process (Nowell, Norris, White, & Moules, 2017).

The interviews were conducted, transcribed and analysed by the authors. The coding and theme identification processes in our analysis were data-driven and based on the raw quotes of the interviewees rather than the researchers' own impressions and interpretations. The coding process was performed both manually, through repeated reading of and making notes on interview transcripts, and through the qualitative software NVivo. The codes, and the related extracts, were then organised in overarching themes to ensure that the final thematic map is well-aligned with the research objectives of the study. To ensure reliability and reduce any analyst-generated bias that could be linked to a single researcher, the three authors analysed the data independently for the coding stage and then compared and synthesised their independent coding analyses to create a single "bigger-picture" narrative. During the synthesis procedure, we developed a consensus on the codes that were eventually the building blocks of our themes through exhaustive discussion; this thorough approach in determining the key topics underpinning the research and our systematic analysis framework as a whole increases the validity of our work by reducing individual research biases since the authors acted as checks and balances to each other. During the theme identification process, it was observed that some of the themes might have dimensions that may be overlapping to some degree while a few quotes might underpin more than one theme. This is not a problem though since Braun and Clarke (2006) suggest that the themes and way these relate to each other do not have to smooth out or ignore but instead retain the tensions and inconsistencies within and across data.

### 3.4. Interviewee characteristics

In total, 36 specialists were interviewed. The sample size is consistent with the best practice literature. Baker, Edwards, and Doidge (2012), when examining sampling in qualitative research as a means of answering how many interviews are enough, concluded that a sample between six and twelve interviews may offer extremely valuable findings and represent adequate numbers for a research project that studies hidden or hard to access populations such as elites. Our study's sample size is large enough to provide diversity of perceptions.

Seventy-eight percent of respondents had a title of Dr or a Professor. Nearly 90% of the participants occupy senior, management and board level positions. Thirty-one people are working in Europe, three in the US and two in Asia. Responses were submitted by a mixture of experts, including people working in local authorities, trade associations, transport operators, automotive and connected technology businesses, non-governmental organisations and universities conducting CAV research. The interviews were male-dominated; we had only seven female participants. According to a Forbes (2010) report, 95% of the National Automobile Association members are men. Also, the tech industry has always been male-dominated at all levels being considerably worse than non-tech industries.

Table 2 lists some key characteristics of the sample providing information about the participants. The code representing each interviewee consists of a field identifier (CO for consultants, IN for automotive or technology industry, OR for non-governmental organisations, GO for government and AC for academics) and a number for each participant within this group.

## 4. Results and analysis

Six core themes emerged during our analysis; these are all critical issues that need to be addressed prior to a full-scale launch of CAVs. Specifically, the themes are: *awareness*, *user and vendor education, safety*, *responsibility*, *legislation*, and *trust*. Each of the themes has diverse and distinctive dimensions that for the means of this study are reported as sub-themes. We acknowledge that some of the themes and their underpinning dimensions may overlap to some degree.

### 4.1. Overview of findings

As this is an elite interview process, all our respondents have knowledge or experience in at least one of our key areas referring to cyber security, privacy and CAVs. During the interview, the participants were asked to provide their opinion on cyber security and privacy in regards to challenges reflecting and affecting CAV technology. It should be noted that although each participant was provided freedom to express one's own views (both positive and negative), the questions directed them to provide their opinion on the problems and challenges, which are primarily negative in nature. A major overarching topic discussed by the experts is the importance of protecting individual privacy and cyber security from criminal and malicious attacks. In the subsections below, themes are presented and evidenced through the presentation of selected relevant quotations. This is one of the most effective and objective ways of delivering a concrete thematic analysis (Nikitas et al., 2019).

### 4.2. Awareness

In information security, awareness refers to the ability of the user to recognise or avoid behaviours that would compromise cyber security. Users' awareness is identified as a key element of sensitising them on CAV-related issues and empowering them to obtain sufficient knowledge on what CAVs and related systems are doing and sharing. Awareness of IT systems

has long been a challenging problem in regards to security, as when users have insufficient awareness, they are likely to put themselves at unnecessary risk. Many respondents expressed the view that limited user awareness will be a source of problems associated with CAVs, so raising awareness about privacy and cyber security issues is of critical importance.

*"CO2: Customers also have a responsibility to be aware about privacy and cyber security and keep up with at least the consumer level knowledge of CAVs."*
*"CO1: Even if the technology part of CAVs is perfect, humans will put themselves in risk by not knowing how to operate the CAV in the right way."*
*"AC2: User awareness is not supported with the right tools and training and thus is an issue."*

Understanding the vulnerability of CAV systems is a crucial aspect of user awareness; knowledge on cyber security and conscious conduct should be promoted in schools and societies in general, in order to minimise cyber attacks based on human error.

*"OR3: I think cyber security knowledge should be taught in schools from elementary school."*
*"AC5: So what the end user can do is to be more aware of the potential consequences when engaging in activities with possible cyber security and privacy consequences"*

As with other fundamental rights, privacy can be taken for granted, therefore, lack of awareness about privacy could result in the exposure of sensitive information.

*"CO4: Ideally we would expect the user to be aware of what personal data is and how it can be used against them. They need to know how to protect themselves."*
*"AC8: CAVs have the ability to store and transmit data. This creates privacy concerns that personal information of CAV users may be misused by external companies, for reasons such as advertising, profiling and tracking their location Users should be aware of this risk."*
*"GO3: A lot of people have these privacy concerns, but at the same time their behaviours, sparked from unawareness, are essentially giving up their privacy rights."*

Although in most cases, the user often ignores the detail of consumer notices and consent, the role of such documentation will continue to be important and essential. However, new mechanisms of informing the user may be required to improve the rate and quality of knowledge transfer. Many respondents pointed out that it is vital to inform the user about the potential options referring to user consent, and about their respective benefits and risks.

*"IN1: Informing the user about the terms and conditions of CAV use and the risk involved is important, but nowadays that is more of a design issue."*
*"GO1: Customer consent is not sufficient to ensure data privacy as most customers simply accept the terms and conditions without fully reading or understanding them."*
*"AC4: Those responsible for CAVs need to come up with some kind of a model or a mechanism to ensure that the drivers are made aware of when their consent is obtained before any data is collected and exploited."*
*"AC13: I think you are going to have people agreeing to the terms and conditions and being unaware or uninformed of the extent to which their personal data is being used for other purposes."*

Some respondents highlighted the importance of designing and offering user-friendly Human-Machine Interface (HMI). It was suggested that efforts to integrate these services would result in better user experience, and it could prevent users from accidentally engaging in cyber attacks and data breaches.

*"AC9: It's rare for people to work their way through the menu from page one. So it's about providing an interface that allows people to understand what is happening. Whereas, if let's say I had a car with really good natural language interface, I would just ask my car, 'what is that flashing icon on the dashboard', and the car would say, 'that is ABC', and I will go okay."*

### 4.3. User and vendor education

According to learning theories and learning continuum hierarchy, education is distinctly interlinked with creating and increasing awareness to the members of the public (Christiansen & Piekarz, 2019). The purpose of raising awareness intends to enable individuals to recognise security problems and act accordingly, whereas education focuses on the knowledge or skill obtained or developed by a learning process (Wilson & Hash, 2003). User and vendor education is a theme expressing that all people involved with CAVs, regardless of whether they are end-users or manufacturers, should be educated on CAV functionality. Education is necessary as a tool enabling the end-user to better prepare and protect oneself, fellow passengers, and the CAV against cyber security threats and ensure that an appropriate standard of privacy is provided.

Several respondents highlighted the importance of user education as well as up-to-date vendor education.

*"CO3: It is vital to educate the user of this new technology and the risks associated with it."*
*"IN4: The vendors do not give any introduction of the car, all they care about is the sales."*

*"AC3: The vendor education is important too, if they do not know anything about the risks embedded in the use of CAVs, then who will warn the user?"*

Another dimension underpinning the theme of education refers to knowledge supply, with some responses highlighting the problems that lack of information or excess of information might cause to the user. Literature showed that an overload of information could cause analysis paralysis (Stanley & Clipsham, 1997) and information fatigue syndrome (Oppenheim, 1997). Although the developers of software systems might be aware of these issues, the consequences when considering CAVs are high, and it is believed that supplying succinct knowledge at the right level is essential for the end-user.

*"AC16: At least from my experience, I wasn't given any information about the connectivity of the car."*
*"IN6: A user might be faced with a thousand-page CAV menu, which he or she has got to hang through, to try and find the relevant bits."*

It was suggested that the automotive industry and all stakeholders should promote CAV education. Campaigns, workshops, and trials are needed to disseminate best practice and support decision-making knowledge.

*"IN3: CAV education should be available not just in the school level but also in TV ads, billboards and everywhere."*
*"AC1: I think workshops could be very helpful. These will help people to understand what the different range of vehicles might be, and what the impact on their lives will be, both positive and negative. CAVs are a disruptive technology, so there will be winners and losers."*
*"GO2: So, for children to understand what data mean, the trade bodies need to look after the advertising and making sure that there is no misguiding advertising."*

All respondents felt user-centred education should be an investment priority for the CAV industry. Many respondents mentioned that governments should also take on the role of facilitating future CAV education for the user, as well as supporting investments improving their current technology.

*"GO2: I think user-centred education should be an investment priority for the CAV industry and the policy-makers."*
*"AC12: You don't always have to change the person per se sometimes you can change the system and the training provision."*

A specially designed CAV driving license was also suggested as a means of ensuring people behave in a desired way, whereby the person does not pose a risk to one's or any other persons' safety and privacy through lack of correct cyber security practice.

*"IN1: School education should support CAV training. In the end we should create a driving license programme that everyone should take to guarantee that they are knowledgeable enough to use CAVs responsibly. This is important based on the fact that the whole society is impacted by this technology."*

### *4.4. Safety*

Safety was identified as one of the primary factors defining the end-user adoption potential of CAVs by most of our interviewed experts. Specifically, our respondents raised concerns about the existing level of cyber security and privacy in CAVs and how these may link to safety. Making sure that hacking and exposing users to unsafe situations would be avoided at any cause were highlighted as two key priorities for the automotive manufacturers.

*"IN3: It'll be up to the car manufacturers themselves and then car clubs and eventually users to know that a CAV is safe. They will have to prove it by testing thoroughly its safety. It is not a game like the one where Top Gear people trying to hack into cars. Safety comes first."*
*"AC15: One of the key steering points of CAVs is safety; one of the key challenges of CAVs is also safety."*

A recurring view was the increasing need to develop skills in cyber security and privacy, across both industry and local authorities for responding to unexpected circumstances. Having a new type of driving license as a compulsory prerequirement for being allowed on a CAV that would assess and ensure the user's ability to manage safely the potential risks of such a vehicle was considered by some interviewees as a critical safeguard mechanism for the technology.

*"AC6: Today we are driving a car that is not fully automated and very different from a CAV. In order to legitimately operate a fully automated car, you must have a driving license specifically for it. This is an enforcement measure which solidifies that you should have a certain level of skills and safety understanding in order to operate CAVs and lessen risks."*

Another point concerning safety which has already been heavily discussed in the field and was mentioned in the interviews are edge cases; situations that happen very rarely and indicate that there will always be unforeseen circumstances in future scenarios.

*"AC9: For future level four or five vehicles is how to deal with what's known as edge cases, situations that happen very rarely, that they can't necessarily be predicted by the programmer. This means that they're not necessarily understood by CAVs. This car can thus be a hazard."*

Furthermore, a number of respondents reported that a better understanding of the user behaviour during a crisis situation was needed.

*"OR2: What is the behaviour of people in crisis situations? How to classify and analyse these behaviours is a new problem we need to face."*

A similar number of respondents raised the need to improve sustainability, accessibility and safety targeting older people or those with disabilities in order to achieve transport equity.

*"IN5: CAV technology should deliver real benefits, in terms of sustainability, access and safety particularly for young, older and disabled people."*

### 4.5. Responsibility

Involving the end-user was also mentioned as a critical factor in ensuring novel transport solutions would be adopted. Respondents frequently felt that the end-user should take responsibilities for the human error accrued. There is an overlap here with liability, as ensuring the end-user understands what they are liable for will help them to act more responsibly.

*"GO4: Humans are the leading cause of AV accidents in California."*
*"AC7: It's just about whether or not certain people basically abuse the system, by getting control of the vehicle in some shape or form and then using that control in a potentially negative way."*
*"AC4: The usual kind of responsibilities or roles that we expect them to be mindful of, in the present environment for security, I think they apply to CAVs as well."*
*"CO2: Because I know I'm responsible for the car itself, but also for safety, or for the data that I have, for other users of the car I need to be extremely mindful. I think that responsibility of use is a feature critical for making CAVs a success."*

Many of the respondents suggested that collaboration between CAV industry, academia, local governments and non-governmental organisations should be encouraged. It was felt that this would increase the chances of projects leading to new business models that solve real cyber security and privacy problems in CAVs. All stakeholders would need to share and define the CAV-related responsibilities.

*"CO3: All of the parties involved have certain very important responsibilities. The government has to set up an education system to inform consumers. The users themselves should behave responsibly when on a CAV. Industry has the responsibility for ensuring sufficient engagement between all the important actors of a CAV transition."*
*"AC10: I think it should be a joint effort when it comes to responsibility. Because it should not be just the car manufacturer and the car manufacturer's responsibility but also the users."*
*"OR3: I guess technically the manufacturers don't have to educate the user, but I think it is the morally correct thing for them to do."*

Respondents emphasised the need to clarify the responsibilities and roles that each stakeholder plays within CAV operations. Establishing a universal framework for ethics when using CAVs that allocates responsibilities when accidents occur is another dimension that underpins this theme according to our findings and is in line with the literature (Borenstein, Herkert, & Miller, 2017; Hevelke & Nida-Rümelin, 2015).

*"CO3: Things like 'if someone's died whose responsibility is this?' need to be better defined. This is a complex responsibility that may lie with the law-maker, decision-makers in the government and also reflect the duties of the involved industries."*

### 4.6. Legislation

To enable the widespread use of CAVs, it was often stated, that more regulatory and legislative efforts need to be conducted. Several respondents stressed the need for legislation focused on CAVs in general and cyber security and privacy in CAVs in particular. These interviewees emphasised the need that legislation should be established before the implementation of infrastructure. This is necessary as adding legislation in a reactive manner may be less effective at protecting citizen's privacy and well-being.

*"CO1: It is necessary to have regulations in place about how companies have to communicate."*
*"AC14: Some of this transition is down to government in terms of regulation. Regulation and licensing need to make sure that the key stakeholders have everything in place when it comes to CAVs to inspire and enable trust."*
*"IN4: Legislation needs to be ready first, and cyber security and technology communities need to understand to what extent the legal protection should be provided for CAVs"*

Recommendations included ensuring CAV drivers and relevant technicians at all levels (such as those working in the manufacturing, maintenance, vendor industries) will be required by law to be fully qualified. Also introducing a specially designed driving license programme that improves the skill set of those involved with CAV-handling duties, particularly with respect to digital skills and awareness of cyber security and privacy was deemed critical. Our interviewees also highlighted the need for the creation of technology-neutral industry codes and standards.

*"AC4: In the industry, there is little debate and little understanding in terms of any agreements or standards or any consensus around this (driver and vehicle standards). Legislation should be able to clear things up and set the standard that would allow the use of CAVs to be genuinely secure. Licenses for qualified users should be legally enforced."*
*"IN6: A consensus is needed between the stakeholders that will lead to the standardisation of CAVs in legal terms too."*

A clearer and more accurate assessment of the likely distribution of liabilities need to be allocated. This would help encouraging the stakeholders in CAV industry to have the confidence to take risks where appropriate. At present, it is currently unknown who will have the responsibility of the vehicle's cyber security aspects. This is an issue greater than cyber security, as it is currently unclear who is responsible in the scenario that a CAV is involved in an accident. Would it be the end-user or the manufacturer? This same issue translates into concerns that might occur from a cyber attack; will the software developer become a potential candidate for sharing liability if a cyber attack is successful? The uncertainty regarding liability concerns amongst experts is evident in their reported opinions.

*"AC5: A good assessment of risk and vulnerabilities should be critical and thus need to be demanded by legislation. Online behaviours that might be accessible to CAV companies need to be screened. The software developers need to have in place tools for identifying and assessing cyber security dangers. Driving insurance companies should play a role in this risk evaluation process."*
*"AC8: As the human is no longer in control of the AV, at least some responsibility and liability for accidents involving AVs will shift to the AV system and the third parties who designed and operated them, necessitating reviews of liability laws to clearly delineate different responsibilities among all AV stakeholders"*

Prohibiting design error from the product-development process would reduce the risk of privacy and cyber security breaches. Many responses discussed the *Privacy by Design* and *Cyber security by Design*, with an emphasis on the need for more inclusive and thoughtful design that could be used as an enforcement scheme. As previously mentioned, there is an overlap between privacy by design and privacy by default; however, privacy by design extends beyond the default privacy sharing policy and is focused on ensuring the underlying software and hardware architectures take all reasonable steps to preserve privacy, which includes aspects such as data minimisation, encryption and secure storage mechanisms.

*"AC11: Focusing on the customer sits at the centre of every management model out there, but design thinking takes it one step further. It places the user at the centre of the solution."*
*"OR3: It's not the car that's providing the security. It's the people who design the car systems and then those that use them."*
*"IN1: I think this comes down to a design principle. According to the conversation we're having with some of our partners, one of the critical issues with privacy and cyber security is that CAVs should be designed to be safe and mitigate the risk of attacks both physical and cyber security by default."*

Respondents called for a discussion on the need to explore a privacy option (such as privacy by default) that could be applied to all, as all devices need to be secure without much intervention by the users who may have limited knowledge about privacy. There is an overlap here with the aspects of the European legal framework of GDPR, where privacy by design is a core principle. This is a challenging aim, as enforcing strong privacy requirements often results in reduced or restricted end-user functionality, and thus the trade-off between privacy and functionality in default configurations needs careful consideration.

*"AC5: I'm sure there are bigger and better ways of ensuring security that I'm unaware of, but having them set as a default, which seems not to be the case, it is a clear way to ensure that the data is only used for the intended purpose and by its intended end-users. So, I would say that probably this is an important step towards the right direction."*

### 4.7. Trust

To fully accept and harness CAVs, it is necessary that end-users trust CAV technology. Trust is another key concept in vehicular networks and underpins acceptability as this is registered by attitudes. Substantial empirical evidence shows that automation faults cause a decline in trust (Lee & See, 2004). One way to cope with public acceptance is to employ social trust when assessing the risks of a new technology (Siegrist & Cvetkovich, 2000). In other words, acceptance of, or willingness to use CAVs, is directly determined by the trust on CAVs.

*"IN1: If a cyber security or privacy breach causes a safety problem, that's going to create serious trust problems. Safeguarding privacy and cyber security will eventually mean improved trust and thus improved acceptance for CAVs"*
*"CO5: User acceptance will be heavily influenced by trust on CAVs as well as the legal frameworks."*
*"IN7: I think the CAV industry must make important investments on building user trust."*

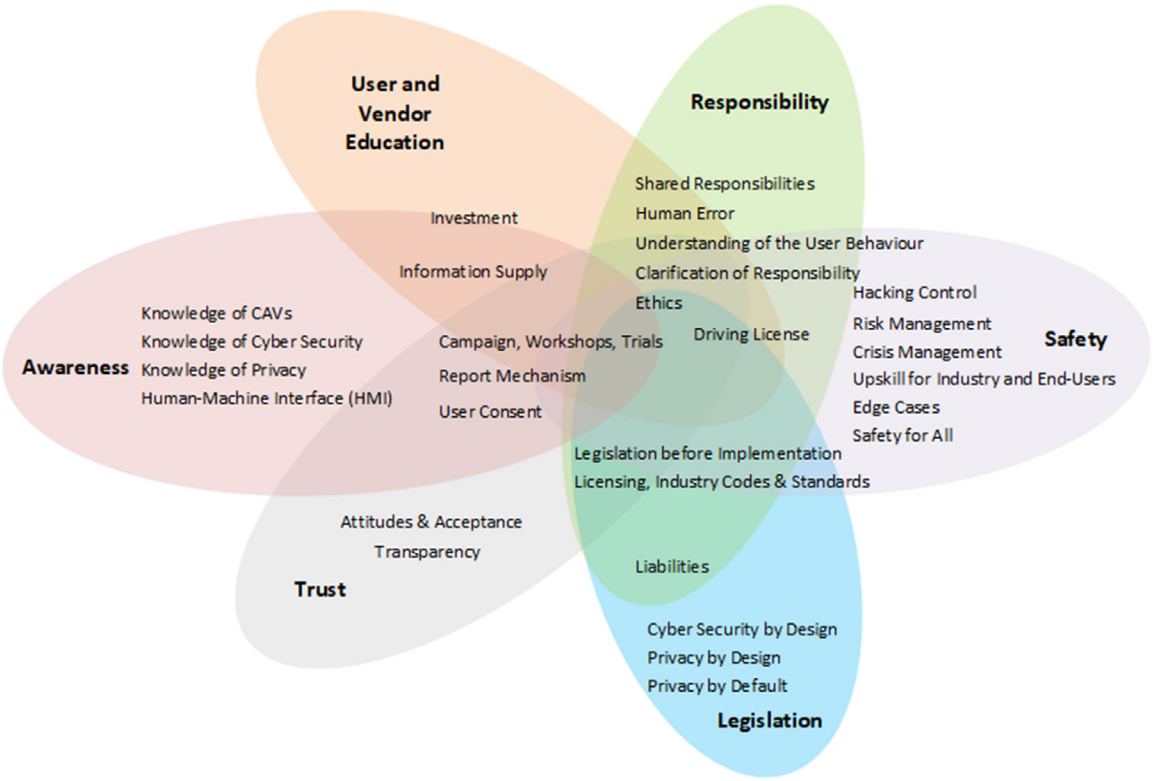


**Fig. 1.** A thematic conceptualisation of the cyber security and privacy issues underpinning CAV acceptance.

Trust could be built up through campaigns, workshops and trials to ensure the CAV users feel comfortable and confident with them.

*"CO3: If people come closer to CAVs through social media, advertising and campaigns, and then really get the experience of a CAV for free, their trust regarding this technology may increase dramatically."*
*"AC4: Where there are lots of safety campaigns, they are partly funded by insurance companies, partly funded by government, partly funded by car companies, partly funded by campaign groups. This is exactly what needs to happen in the CAV security domain. We need to learn from these existing models advocating for traffic safety and think about how we can adopt similar models that work for the privacy and cyber security agendas of CAVs."*

Social media play a big role in shaping public views on some issues and influencing the trust building process. To reach a diverse range of audiences, several respondents advocated the use of different means of communication, including information campaigns and the use of social media.

*"OR2: Most of the things which end-users receive about CAVs is coming from social media or the media itself, and that information can be misleading."*
*"OR3: Manufacturers or leasing companies need to better play up the security features in their advertising. They should be providing messages such as 'while you're in an automated vehicle, all of your data we collect will not be associated with your personal data, they are not going to be shared with external parties, everything is totally safe and legitimate'. I think that will help to build trust and it will make people more aware of cyber security and privacy."*

Transparency is always the key element behind trust; this has been heavily examined in literature of transport interventions (e.g. Pettersson & Karlsson, 2015; Ekman, Johansson, Bligård, Karlsson, & Strömberg, 2019). Several respondents raised the need to provide the public with transparent assurance about the safety of CAVs.

*"IN1: Being open about what has happened when things go wrong and about the process that is being followed is a sign about actively looking for ways with which you can overcome challenges and get the necessary help to solve problems. Transparency benefits trust-building."*
*"AC10: Any effort to try hiding what is happening with CAVs will be the worst-case scenario."*
*"OR1: There is not much transparency of what they say and what they are actually collecting."*

*"AC4: Transparency is key, in terms of realising and solving problems whether these are about technical product design and whether these are about legislations and regulations. You need to be honest with the future users as well; people do not like 'games'."*

Having a sufficient and prompt reporting and responding mechanism in place is necessary for creating a communication dialogue between all stakeholder groups. This would help to ensure that the CAV industry and the end-users closely engage with technology and its associated risks, resulting in a confidence increase of the user. It is foreseen that reporting mechanisms will enable two-way communication, providing the potential for manufacturers to supply information of security nature to the end-user (e.g. information on software fixes), and also mechanisms for the end-user to inform the manufacturer of any issues they have noticed or are experiencing.

*"AC11: There should be functions available about reporting where and when things are going wrong. Having a good two-way support mechanism affects positively the end-user."*
*"IN2: I think the challenge of course is that there are so many cases of problems we cannot yet appreciate, but what we don't have, and needs to be adopted before CAVs are fully launched, is a publicly transparent reporting mechanism."*
*"IN5: If we don't have a rigorous transparent way of reporting on threats, failures or attacks and so on, there will be a breakdown of trust between or across the industry."*
*"IN7: Trust depends fundamentally on security. Interactive real-time communication between the user and a control centre will help in this sense."*

### *4.8. A thematic roadmap conceptualising the privacy and cyber security agendas in CAVs*

The interviews revealed six themes that could play a key role, according to our subject experts, in the way people may respond to CAVs when focusing on the privacy and cyber security agendas. These themes are: *awareness, user and vendor education, safety, responsibility, legislation* and *trust.* These are priority areas for the policy, planning, design and manufacturing of CAVs that must be addressed before their full-scale launch so that the transition to a CAV-centric mobility paradigm can be unproblematic. Each of these themes have their own distinctive and diverse dimensions which have been presented one by one in the analysis section and can be listed as sub-themes. Fig. 1 is a thematic framework that brings everything together in a single infographic. It specifically conceptualises the key themes, their sub-themes and the interrelations between them representing a very accurate coding snapshot of the present work. The figure presents occurrences of overlapping acknowledging the links that these theme expressions have with one another and the fact that some key concepts fit and reflect more than one theme simultaneously. Therefore, Fig. 1 ultimately presents an evidence-based roadmap of the opportunities and challenges embedded in the cyber security and privacy agendas of CAVs that may define the public acceptance of this emerging technology.

## 5. Discussion and policy recommendations

This section will further contextualise the six themes and their key sub-themes benchmarking them when possible against relevant literature. It is a discussion that seeks to develop a fluid and recursive frame that elaborates on our analysis being systematic but not rigid. All themes and most of their key expressions are discussed thoroughly but not necessarily in the order outlined in our analysis; this is a synthesis designed to help the reader appreciate better the 'big picture' of cyber security and privacy in CAVs.

CAVs may change the norms in mobility provision dramatically, and as with any other disruptive technology, their public acceptance depends on building trust (Ekman et al., 2019; Nikitas et al., 2019; Zhang et al., 2020). When the public mistrusts politicians, mobility providers, automotive, telecommunication and intelligence industries or CAV operating algorithms, and even begins to suspect that the underlying motivations of the parties involved in this process of transition may be underpinned by hidden agendas like data exploitation to name one, trust will be hard to develop and establish. And if trust is broken it is very difficult to be reconstructed for the context of transportation (Nikitas et al., 2018).

It was suggested by several respondents that building trust could be done through campaigns, workshops, advertisement and test drives; this broad approach can reach a diverse range of audiences. Media are the major player in influencing public opinion by exposing and bringing new technologies under scrutiny daily something that can make the public's trust fragile. Subsequently, the public has become more defensive, demanding that any new technology should be clearly explained. Explanations (i.e. reasons to justify why an action should or should not be taken) in the context of AVs have been found to help trust-building (Du et al., 2019). This makes transparency crucial, therefore, creating the need for manufacturers and policy-makers to become more accountable. This is supported by the view of several respondents, who highlighted the importance of reassuring the public about the ability of CAVs to provide a secure personal space. A number of respondents stressed the importance of transparency regarding the reporting and responding mechanism that needs to be in place to facilitate an open and systematic dialogue between the CAV industry and its end-users. Promoting transparency about what data is collected, including both passive and active data collection, and collecting data in a way that is clear and easy for the user to understand is needed. However, we recognise that transparency is not always achievable or desirable in algorithms. Companies have legitimate trade secrets that they must keep confidential. Transparency can expose the security

apparatus of a company to security risks where hackers and cyber criminals can attack the system. Vulnerability disclosure mechanisms should be established too; a two-way interactive and honest communication should be available in CAVs. In particular, any report or statements made in the event of a cyber security or privacy breach should be as comprehensive and accurate as possible. Through this, the manufacturers will provide genuine information about the cyber security and privacy risks in CAVs, while the end-users will give feedback to the manufacturers regarding safety problems that they will come across, ultimately resulting in building trust between both parties.

Trust on any new technology is inevitably linked to education on the basis that the general public needs to get educated on the dangers that this technology might entail. Cyber security and privacy risks are beyond traditional security risks and as such their consequences may be passively and unconsciously exposed or only impact the end-user long term. Therefore, public opinion on these new digital risks should be treated differently, as the source of threat and danger cannot be easily and clearly identified. It should be noted that most end-users and vendors have limited knowledge to date when it comes to CAV associated risks. Therefore education and awareness enhancement are vital in order to offset the fear that cyber security and privacy risks might generate as a number of respondents suggested. Studies have found that the lack of sufficient knowledge and awareness among key stakeholders and the public is a major barrier to successful risk prevention (Burt et al., 2007; Chang et al., 2009; Cohen, Mirotchnick, & Leung, 2007). Most respondents raised the point that automotive vendors are not well-informed about the potential adverse effects of cyber security and privacy risks to the current level-two AV, which results in the customers not being informed either when they buy the vehicle. We suggest that vendors should receive as a prerequisite for their engagement in this market a very detailed CAV-specific education that allows them to be fully aware and alerted about digital risks. Specific education about cyber security, privacy, code of conduct should be disseminated to the end-user in the purchase or subscription process. Licensing for the independent use of CAVs after a training course may also be a necessary step that will enable avoiding cyber security threats and privacy breaches; our interviewees argued that a well-educated and trained user is always a better user for the context of CAVs. We thus recommend, that specially designed CAV driving license courses should be a compulsory element for the transition to the era of CAVs that will teach the end-users specific security-conscious behaviours, in a simple and actionable way. This type of licensing can eventually replace the current driving license that will not be needed in the era of CAVs; so this will not necessarily impose a new untested usage prerequisite but rather be a modernised continuation of a well-established licensing scheme that will require less skill but may be needed for any independent user of CAVs.

Education demystifying innovative technology is one of the few investments in social programmes that may have a high return on investment (Facer, 2011). All of the respondents supported the idea that education should be an investment priority of the CAV industry, while some also recognised this as a government responsibility. Systematic investment plans equipping professionals and the general public with the right skills could mitigate digital risks and help governments to create more secure societies. Based on the evidence provided herein we suggest that in addition to the government and the automotive industry, Internet, telecommunications and intelligence service providers should take part of the responsibility to educate the end-users about cyber threats and privacy breaches, as they could be the connectivity intermediary that bridges end-users with CAVs. We argue that the elites believe that education is a primary solution to the prospective risks associated with CAVs. However, the elites did not infer that educating users is hard and less effective because privacy and cyber risks are dynamic and constantly evolving. As such, it is difficult to maintain constant educational updates for the users. Also, it would be perhaps more effective and resource-efficient to educate CAV engineers, developers and retailers to avoid introducing security- and privacy-prone systems.

Ensuring an improved level of public awareness about cyber security and privacy issues may be the first step of any education programme. Being aware of a risk or a problem is the stepping stone in looking for and eventually adopting responsible and secure ways of operating CAVs and handling their data. Nowadays, cyber threats and privacy breaches are regrettably common and prevalent (Ricci, Breitinger, & Baggili, 2019). At the same time, governments and businesses are investing heavily in cyber security and privacy solutions (Tao et al., 2019). In Europe, GDPR has shed light on data privacy and has generated substantial awareness regarding some aspects of the problem of personal data collection and export. Yet, public awareness has not been cultivated to the desired extent (Papoutsi et al., 2015). In the case of phishing and ransomware, attacks can lead to the loss of property, whereas in the case of CAVs, they can result in serious injuries or even death. Therefore, it is essential for the public to become aware of its role in cyber security, so that they can understand that their actions matter and make safe choices. As some respondents suggested, this can be achieved via robust HMI, the development of which is crucial. According to the literature, awareness raising programmes will be successful if they are tailored to targeted groups of stakeholders (García-Llorente, Martín-López, González, Alcorlo, & Montes, 2008). Robust HMI will enable the required information to be passed on to the end-user quickly and reliably, enhancing the efficiency of awareness cultivation.

Cyber security and privacy awareness are also linked to issues reflecting and affecting user consent. GDPR requires the personal data to only be collected and retained for *'specific, explicit, and legitimate purposes'*, and only with the user's consent. We argue that the 'signing of terms and conditions' which is nowadays a common practice to transfer responsibility to the user is only a very basic tick-box exercise that cannot be elevated to user consent; this many times actually works as a camouflage technique for shedding responsibility and not as a facilitator of genuine understanding that will reduce errors and mishandling. This is because many people do not read the terms and conditions to which they have assumingly consented (Steinfeld, 2016) many times due to information overload (Obar & Oeldorf-Hirsch, 2020). Moreover, people who have agreed with the terms and conditions for subscribing to a service usually do not understand them, because of the complex legal and

technical terminology used (Tsai, Egelman, Cranor, & Acquisti, 2011). Considering the above, the question of whether the public can consent to things they do not understand arises. We recommend that raising awareness through the means of legally-required education that will be far superior and more extensive than a tick-box exercise will promote genuinely user responsibility. However, at the same time some might argue that the automotive industry has avoided educating the public on the risks of motor vehicles since the 1900s. This might mean that the public would need to get educated to opt for more secure and well-designed products rather than changing their consumer behaviour or attending high-tech training such as those of computer engineers. Legislation should thus be put in place to enforce the good design practice so as to ensure that the end-users are protected from associated cyber risks.

Legislation has many more equally critical dimensions when it comes to CAVs' privacy and cyber security. Legislation is especially challenging when the commercialisation of the end-user's data leads to certain stakeholders making profit while damage is imposed on the end-user. Considering the international nature of cyber attacks, international criminal groups tend to exploit legislation and jurisdictional loopholes (Adamoli, Di Nicola, Savona, & Zoffi, 1998). Therefore, it is essential to create a framework in which software is developed at international standards. In addition, professional organisations need to address the issues of accreditation and recertification in a modern way in order to keep up with the continuous changes in the industry. Furthermore, without the necessary legislation in place, the CAV market could potentially fall into what is known as a 'lemon market' in economics, where manufacturers compete only on features that consumers can perceive, ignoring the ones they do not, such as cyber security and privacy. If in the long run CAVs with poor cyber security and privacy standards dominate the market, market failure could arise, resulting in a loss of social welfare. Also, as Nunes, Reimer, and Coughlin (2018) highlighted, exempting developers from safety rules poses risks; if developers are not always required to report system failures or to establish competency standards for vehicle operators, legislation should penalise them. Favouring industry over users will erode support for the technology from an already sceptical public. Legislation should also not sidestep the education of consumers; standards of competency and regular proficiency testing for users should be shaping consumer education programmes.

The complexity of the CAV system makes it particularly difficult for its security to be ensured. A higher degree of complexity can potentially lead to the occurrence of an increased number of errors in the design and development process, as well as to the greater difficulty in testing, consequently making *Security by Design* and *Privacy by Design* vital. Starting from the earliest manufacturing stage, the design process, up until the final manufacturing stage, the commercialisation of the technology, the CAV industry should be highly regulated and forced to follow certain principles. Several respondents suggested that the liability law should be improved by setting rules which aim to punish misconduct. In GDPR, executives and board members could face liability for data breaches (EU GDPR Portal, 2018). UK launched the *Secure By Design, Secure by Default: Self-Certification Scheme*[1] in 2019, to ensure the UK's resilience against different forms of cyber security vulnerability. However, whether this law-like approach fulfils effective regulatory design criteria remains unexamined. Therefore, it is of utmost importance that the liabilities of all different parties, including the end-user, should be clarified. Furthermore, there has to be a certain limit of liabilities that should be in place, otherwise the development of new technologies will be suppressed. The UK government is an example of a government that chooses to apply relatively soft policies when it comes to liabilities in the CAV industry. UK does not currently contain any specific provisions relating to user liability; Law Commission (2018) has suggested that the legislation must be developed further to clarify the role of the 'user-in-charge'. Upcoming legislation is being prepared based on the security-by-design principle in the UK since the start of 2020. We argue that a middle ground, between a heavily regulated industry and an uncontrolled one, has to be found. Maybe it would be more reliable for the insurance market to be encouraged to leverage the risk. Insurance is a self-reinforcing mechanism for improving security and safety, while still allowing companies room to innovate (Schneier, 2018). As a whole, user-friendly legislation clarifying responsibility, liability disputes, manufacturing and commercialisation procedures, educational programme prerequisites and creating a generic regulatory framework of operation should be in place before the implementation of CAVs (Nikitas et al., 2019) and should focus, with special care, on privacy and cyber security issues.

Often the required cyber security and privacy configurations are tedious and complicated, and beyond the skill of the average end-user. There is also a lack of clearly defined lines about how end-users are expected to behave when they experience a cyber attack or a crisis situation. As discussed in legislation, attribution can be difficult. Our respondents suggest the end-user should also take some responsibilities for any human error that occurs when a CAV operates. In 2014, Microsoft drafted *International cyber security norms*, which introduced a set of norms for acceptable behaviour in cyberspace; this could be an inspiration for defining what a responsible CAV behaviour is. The complex nature of the CAV technology will require inter-institutional cooperation, the exploration of relevant human behaviour modelling, a commitment to incremental interdisciplinary initiative development, a solid ethical framework and consensus on threats and appropriate actions to manage CAVs and their associated risk.

Safety is a core prerequisite to any IoT device and thus critical for the acceptance of CAVs. Our respondents clearly highlighted that cyber security threats and privacy breaches would be viewed as inadequate safety provision by most end-users. Since safety has been the prime reason for introducing the CAVs in the first place and is the most critical criterion for their perceived success (Hulse, Xie, & Galea, 2018; Papadoulis, Quddus, & Imprialou, 2019) and privacy and cyber security have clear links with safety perceptions (Taeihagh & Lim, 2019), prioritising CAV solutions that address these concerns would

[1] See the scheme online: https://www.gov.uk/government/news/secure-by-design-secure-by-default-self-certification-scheme-launched.

be a decisive step towards the right direction. Ensuring the safety of CAVs, according to Koopman and Wagner (2017), requires a multi-disciplinary approach from all the involved stakeholders across all the levels of functional hierarchy including activities looking to support: hardware and software fault tolerance; resilient machine learning; cooperation with human-driven vehicles; validation systems for operation in highly unstructured environments; and appropriate regulatory approaches. In regards to the edge cases, the most well-known solution is probably *prototyping*, where researchers and developers can simulate unsafe situations arising from cyber security and privacy threats to explore crisis management solutions (Brugali et al., 2014).

## 6. Limitations and future research

While this is a rigorous qualitative work, that followed a systematic data collection and analysis approach in line with best practice in qualitative research the authors acknowledge that there are limitations in their study. Braun and Clarke (2006) argue that a strong thematic analysis does not necessarily focus on following procedures "correctly, accurately, or reliably" or achieving a perfect consensus between coders. Rather, it focuses on the researcher's reflective and thoughtful engagement with both the data and the analytic process. In general, we agree with Braun and Clarke that there is no one single way of analysing the data, because it is impossible for the researchers to avoid ontological, epistemological and paradigmatic assumptions. Coding will always reflect the researchers' philosophical standpoint and research values, while reliability measures only confirm that the three independent analysts, have coded the data in the same meticulous way. We have adopted the Braun and Clarke's six-step thematic analysis approach which seeks to develop a fluid and recursive frame which is different from the rigid and structured frame that the traditional codebook approach typically uses but at the same time we used a consistent interview guide and the synthesis of three independent analyses as our reliability measure to improve the coherence and validity of our study. This was a systematic, intensive and insightful interpretative approach that reduced to a considerable degree inconsistencies and potential individual researcher biases. We thus actively combined two schools of qualitative thought following the line of conduct of our previous work (Nikitas et al., 2018, 2019).

We should not also ignore that elite interviews do not necessarily represent the acceptance of users per se; distinctive differences of opinions are bound to exist between the two groups. What the elite interviewees think does not make it the case so the reader should be aware of the difference between our data set and the phenomena studied. We also acknowledge that the elite voices reported from industry, academia and policy speak their own truth and are not privileged to report the unbiased universal reality. We need to recognise that most of the respondents being employed in senior positions in jobs heavily involved in one way or another with CAV-related agendas could make some of their opinions more prone to bias favouring CAVs. Furthermore, it should be acknowledged that our interview guide might not have been able to capture, despite our efforts, all the diverse dimensions of these multi-faceted phenomena examined meaning that some areas could still be relatively unexplored.

The small participation of female respondents although representative of the male-dominated field of CAVs may also generate some bias. Moreover, this study focused primarily on elites from the UK. The sample size (i.e. the small number of participants) and the qualitative nature of the study per se might restrict the generalisability of our findings to a much broader context.

However, the use of elite interviews is beneficial for the policy and planning of CAVs as the emphasis of the research was on privacy and cyber security issues that are at present very specialised topics not common to the average future end-user. The general public is still not particularly exposed to the privacy and cyber security specifics of CAVs, despite some media coverage, and might not have adequate knowledge, answers or sufficient understanding on the subject.

Future research should consider gauging responses from a more balanced international sample. In this regard, the study should test and compare the context of different countries, geographic regions and evaluate the country-specific characteristics of the issues associated with CAVs. Our focus on user acceptance makes it necessary to extend our research focus, beyond elites and their perceptions of privacy and cyber security, and explore public opinions. Despite their limited engagement with CAVs the average future user may have different things to report on this topic. Thus, our follow-up research is looking to explore through the means of a quantitative survey, based on the themes discussed and contextualised herein, the general public attitudes towards the privacy and cyber security issues of CAVs. This next work that is already underway will address this study's key inability, due to its qualitative nature and elite-based character, to generalise some of our results to a much broader context.

## 7. Conclusions

This work addresses the lack of previous research aimed towards understanding the factors underpinning the user acceptance of CAVs when considering cyber security and privacy issues. For this purpose, 36 elite interviews were conducted with field experts from academia, industry and policy-making who provided a diverse and interdisciplinary pool of well-informed insights that enabled the identification and contextualisation of the challenges and opportunities associated with the cyber security and privacy risks of CAVs. Six core themes are identified as elements that could impact acceptance and ultimately adoption potential, namely: *awareness*, *user and vendor education, safety*, *responsibility*, *legislation*, and *trust*. Each of these themes had a number of distinctive dimensions and orientations listed as sub-themes. Since, sooner or later CAVs will be

eventually launched in a large scale we argue that these areas that are now severely overseen and understudied, especially in qualitative terms, need to be prioritised when designing the future of mobility systems. The cyber security and privacy dangers of CAVs can only be mitigated if all the key stakeholders (i.e. the CAV manufacturers, intelligence providers, regulators and end-users) thoroughly understand the opportunities and risks associated with them and work pro-actively together sharing responsibilities instead of allocating faults to one another. Trust should be built by developing testing trials and awareness campaigns that will expose the public to CAVs and their digital risks. More importantly, legally required education that will lead to CAV user licenses will ensure that end-users are informed and trained to behave responsibly and erase human error when riding a CAV. Improving the education and awareness of vendors on this dual agenda is equally, if not more, important. Favouring industry over users should not be an option either; reporting system failures, improving two-way interaction, establishing competency standards, going far beyond the 'term and conditions' education provision methods should be regulated and standardised. Manufacturers at the end of the day will need to create more secure CAV products.

## CRediT authorship contribution statement

**Na Liu:** Conceptualization, Methodology, Data curation, Formal analysis, Writing - original draft, Writing - review & editing. **Alexandros Nikitas:** Conceptualization, Methodology, Formal analysis, Supervision, Writing - original draft, Writing - review & editing. **Simon Parkinson:** Supervision, Formal analysis, Writing - review & editing.

## Acknowledgements

The authors would like to thank Huddersfield Business School and the Artificial Intelligence Research Funding initiative of the University of Huddersfield for their generous funding.

## Appendix A. Interview guide

1. What information will CAVs collect from the user?
2. Will CAVs provide a sufficient level of privacy?
3. What classifies as a breach of privacy for the CAV environment?
4. What can CAV manufacturers do to ensure personal space and privacy?
5. How important is privacy for CAV users and CAV manufacturers?
6. What are the measures that could help the user achieve a 'more private' CAV environment?
7. How the user can help with the task of safeguarding one's privacy when using a CAV?
8. How do you define cyber security?
9. What does cyber security security mean to ordinary people?
10. What an attacker can do to a car if he/she was able to communicate on CAV's internal network maliciously?
11. What is the current state of cyber security and what are the trends for the future regarding cyber security in CAVs?
12. Does the industry and other stakeholders understand how cyber threats evolve and how to anticipate them? What do you (or suggest to) do to avoid them?
13. What should be done before we introduce CAVs into the market?
14. Will engineers/technology providers/regulators be able to solve most modern cyber security problems in AVs?
15. Who exactly is responsible for these problems?
16. How can the user help with the task of safeguarding one's cyber security when using a CAV?
17. How CAV acceptance could be undermined by cyber security and privacy flaws?
18. How can we maintain or inspire trust?
19. What are the common cyber security and privacy mistakes users make?
20. What skills should the user of CAVs have from a cyber security and privacy point of view?
21. What type of education should be provided to CAVs users?
22. What is the role/responsibilities of end-user for CAVs?
23. Who should provide user education for CAVs and how?
24. What is the advice we give to end-users? To what extent do you think they can understand it?
25. How can we promote user responsibility?

## References

Abraham, H., Lee, C., Brady, S., Fitzgerald, C., Mehler, B., Reimer, B., & Coughlin, J. F. (2017). Autonomous vehicles and alternatives to driving: Trust, preferences, and effects of age. *Proceedings of the Transportation Research Board 96th Annual Meeting (TRB'17)*.

Aceto, G., Persico, V., & Pescapé, A. (2019). A Survey on information and communication technologies for industry 4.0: State-of-the-Art, taxonomies, perspectives, and challenges. *IEEE Communications Surveys & Tutorials, 21*(4), 3467–3501.

Acquisti, A. (2004). Privacy and security of personal information. In *Economics of Information Security* (pp. 179–186). Boston, MA: Springer.

Adamoli, S., Di Nicola, A., Savona, E. U., & Zoffi, P. (1998). *Organised crime around the world* (p. 49). Helsinki: Heuni.

Alyavina, E., Nikitas, A., & Njoya, E. T. (2020). Mobility as a service and sustainable travel behaviour: A thematic analysis study. *Transportation Research Part F: Traffic Psychology and Behaviour, 73*, 362–381.

Anderson, J. M., Nidhi, K., Stanley, K. D., Sorensen, P., Samaras, C., & Oluwatola, O. A. (2014). *Autonomous vehicle technology: A guide for policymakers*. Rand Corporation.
Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.
AU, A. K. M, & Enderwick, P. (2000). A cognitive model on attitude towards technology adoption. *Journal of Managerial Psychology*.
Bagloee, S. A., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies. *Journal of Modern Transportation, 24*(4), 284–303.
Baker, S. E., Edwards, R., & Doidge, M. (2012). How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research. National Centre for Research Methods Review Paper.
Bauer, G. S., Greenblatt, J. B., & Gerke, B. F. (2018). Cost, energy, and environmental impact of automated electric taxi fleets in Manhattan. *Environmental Science & Technology, 52*(8), 4920–4928.
Bonnefon, J. F., Shariff, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. *Science, 352*(6293), 1573–1576.
Borenstein, J., Herkert, J., & Miller, K. (2017). Self-driving cars: Ethical responsibilities of design engineers. *IEEE Technology and Society Magazine, 36*(2), 67–75.
Bou-Harb, E., Lucia, W., Forti, N., Weerakkody, S., Ghani, N., & Sinopoli, B. (2017). Cyber meets control: A novel federated approach for resilient cps leveraging real cyber threat intelligence. *IEEE Communications Magazine, 55*(5), 198–204.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.
Brugali, D., Broenink, J., Kroeger, T., & MacDonald, B. (2014). *Simulation, Modeling, and Programming for Autonomous Robots: 4th International Conference, SIMPAR 2014, Bergamo, Italy, October 20-23, 2014. Proceedings* (Vol. 8810). Springer.
Burt, J. W., Muir, A. A., Piovia-Scott, J., Veblen, K. E., Chang, A. L., Grossman, J. D., & Weiskel, H. W. (2007). Preventing horticultural introductions of invasive plants: Potential efficacy of voluntary initiatives. *Biological Invasions, 9*(8), 909–923.
Cavoli, C., Phillips, B., Cohen, T., & Jones, P. (2017). *Social and behavioural questions associated with Automated Vehicles A Literature Review*. UCL Transport Institute January.
Chang, A. L., Grossman, J. D., Spezio, T. S., Weiskel, H. W., Blum, J. C., Burt, J. W., ... Grosholz, E. D. (2009). Tackling aquatic invasions: Risks and opportunities for the aquarium fish industry. *Biological Invasions, 11*(4), 773–785.
Christiansen, B., & Piekarz, A. (2019). Global cyber security labor shortage and international business risk. IGI Global. http://doi:10.4018/978-1-5225-5927-6.
Clark, B., Parkhurst, G., & Ricci, M. (2016). *Understanding the socioeconomic adoption scenarios for autonomous vehicles: A literature review. Project Report*. University of the West of England Bristol.
Clements, L. M., & Kockelman, K. M. (2017). Economic effects of automated vehicles. *Transportation Research Record, 2606*(1), 106–114.
Cohen, J., Mirotchnick, N., & Leung, B. (2007). Thousands introduced annually: The aquarium pathway for non-indigenous plants to the St Lawrence Seaway. *Frontiers in Ecology and the Environment, 5*(10), 528–532.
Cohen, S. A., & Hopkins, D. (2019). Autonomous vehicles and the future of urban tourism. *Annals of Tourism Research, 74*, 33–42.
Cohen, T., Jones, P., & Cavoli, C. (2017). *Social and behavioural questions associated with automated vehicles*. London, UK: University College London Transport Institute Report.
Collingwood, L. (2017). Privacy implications and liability issues of autonomous vehicles. *Information & Communications Technology Law, 26*(1), 32–45.
Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.
Daziano, R. A., Sarrias, M., & Leard, B. (2017). Are consumers willing to pay to let cars drive for them? Analyzing response to autonomous vehicles. *Transportation Research Part C: Emerging Technologies, 78*, 150–164.
Deb, S., Rahman, M. M., Strawderman, L. J., & Garrison, T. M. (2018). Pedestrians' receptivity toward fully automated vehicles: Research review and roadmap for future research. *IEEE Transactions on Human-Machine Systems, 48*(3), 279–290.
Deb, S., Strawderman, L., Carruth, D. W., DuBien, J., Smith, B., & Garrison, T. M. (2017). Development and validation of a questionnaire to assess pedestrian receptivity toward fully autonomous vehicles. *Transportation Research Part C: Emerging Technologies, 84*, 178–195.
Drew, H. (2014). Overcoming barriers: Qualitative interviews with German elites. *Electronic Journal of Business Research Methods, 12*(2).
Du, N., Haspiel, J., Zhang, Q., Tilbury, D., Pradhan, A. K., Yang, X. J., & Robert, L. P. Jr., (2019). Look who's talking now: Implications of AV's explanations on driver's trust, AV preference, anxiety and mental workload. *Transportation Research Part C: Emerging Technologies, 104*, 428–442.
Edwards, M., Nathanson, A., Carroll, J., Wisch, M., Zander, O., & Lubbe, N. (2015). Assessment of integrated pedestrian protection systems with autonomous emergency braking (AEB) and passive safety components. *Traffic Injury Prevention, 16*(sup1), S2–S11.
Ekman, F., Johansson, M., Bligård, L. O., Karlsson, M., & Strömberg, H. (2019). Exploring automated vehicle driving styles as a source of trust information. *Transportation Research Part F: Traffic Psychology and Behaviour, 65*, 268–279.
EU GDPR Portal, 2018. GDPR key changes. Available at: https://www.eugdpr.org/the-regulation.html. Accessed date: 10 February 2020.
Faisal, A., Yigitcanlar, T., Kamruzzaman, M., & Currie, G. (2019). Understanding autonomous vehicles: A systematic literature review on capability, impact, planning and policy. *Journal of Transport and Land Use, 12*(1), 45–72.
Facer, K. (2011). *Learning futures: Education, technology and social change*. Routledge.
Forbes (2010). Transformers: Women And The Automotive Industry. Available online: https://www.forbes.com/2010/05/18/women-auto-industry-influence-forbes-woman-leadership-car-dealers.html#355afdc22e7d
Fraedrich, E., & Lenz, B. (2016). Societal and individual acceptance of autonomous driving. In *Autonomous driving* (pp. 621–640). Berlin, Heidelberg: Springer.
Frewer, L. J., Howard, C., & Shepherd, R. (1998). Understanding public attitudes to technology. *Journal of Risk Research, 1*(3), 221–235. https://doi.org/10.1080/136698798377141.
García-Llorente, M., Martín-López, B., González, J. A., Alcorlo, P., & Montes, C. (2008). Social perceptions of the impacts and benefits of invasive alien species: Implications for management. *Biological Conservation, 141*(12), 2969–2983.
Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., & Kantarcioglu, M. (2017). Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design & Test, 34*(4), 7–17.
Goggin, G. (2019). Disability, connected cars, and communication. *International Journal of Communication* (19328036), 13.
Gössling, S., Cohen, S. A., & Hares, A. (2016). Inside the black box: EU policy officers' perspectives on transport and climate change mitigation. *Journal of Transport Geography, 57*, 83–93.
Hafner, R. J., Walker, I., & Verplanken, B. (2017). Image, not environmentalism: A qualitative exploration of factors influencing vehicle purchasing decisions. *Transportation Research Part A: Policy and Practice, 97*, 89–105.
Hevelke, A., & Nida-Rümelin, J. (2015). Responsibility for crashes of autonomous vehicles: An ethical analysis. *Science and Engineering Ethics, 21*(3), 619–630.
Howard, D., & Dai, D. (2014, January). Public perceptions of self-driving cars: The case of Berkeley, California. In Transportation Research Board 93rd Annual Meeting (pp. 1–16), Vol. 14, No. 4502.
Heard, B. R., Taiebat, M., Xu, M., & Miller, S. A. (2018). Sustainability implications of connected and autonomous vehicles for the food supply chain. *Resources, Conservation and Recycling, 128*, 22–24.
Hohenberger, C., Spörrle, M., & Welpe, I. M. (2016). How and why do men and women differ in their willingness to use automated cars? The influence of emotions across different age groups. *Transportation Research Part A: Policy and Practice, 94*, 374–385.
Hulse, L. M., Xie, H., & Galea, E. R. (2018). Perceptions of autonomous vehicles: Relationships with road users, risk, gender and age. *Safety Science, 102*, 1–13.
Jaremba, U., & Mak, E. (2014). Interviewing judges in the transnational context. *Law and Method, 2014*(2).
Karnouskos, S., & Kerschbaum, F. (2017). Privacy and integrity considerations in hyperconnected autonomous vehicles. *Proceedings of the IEEE, 106*(1), 160–170.

Kaur, K., & Rampersad, G. (2018). Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. *Journal of Engineering and Technology Management, 48*, 87–96.
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134.
Koopman, P., & Wagner, M. (2017). Autonomous vehicle safety: An interdisciplinary challenge. *IEEE Intelligent Transportation Systems Magazine, 9*(1), 90–96.
Kyriakidis, M., Happee, R., & de Winter, J. C. (2015). Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transportation Research Part F: Traffic Psychology and Behaviour, 32*, 127–140.
Lang, N., Mei-Pochtler, A., Rüßmann, M., & Mohr, J. (2015). Revolution versus regulation: The Make-or-break questions about autonomous vehicles. Boston consulting group [online] Available at: https://www.bcgperspectives.com/content/articles/automotive-revolution-versus-regulation-make-breakquestions-autonomous-vehicles. Accessed date: 02 February 2020.
Law Commission (2018). Autonomous Vehicles: A Joint Preliminary Consultation Paper. Available at: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/6.5066_LC_AV-Consultation-Paper-5-November_061118_WEB-1.pdf. Accessed date: 20 June 2020.
Leblanc, R., & Schwartz, M. S. (2007). The black box of board process: Gaining access to a difficult subject. *Corporate Governance: An International Review, 15*(5), 843–851.
Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors, 46*(1), 50–80.
Liljamo, T., Liimatainen, H., & Pöllänen, M. (2018). Attitudes and concerns on automated vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour, 59*, 24–44.
Lim, H. S. M., & Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies, 11*(5), 1062.
Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C. W. (2019). Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Frontiers in Psychology, 10*, 995.
Mamouei, M., Kaparias, I., & Halikias, G. (2018). A framework for user-and system-oriented optimisation of fuel efficiency and traffic flow in Adaptive Cruise Control. *Transportation Research Part C: Emerging Technologies, 92*, 27–41.
Meyer, J., Becker, H., Bösch, P. M., & Axhausen, K. W. (2017). Autonomous vehicles: The next jump in accessibilities? *Research in Transportation Economics, 62*, 80–91.
Milakis, D., Van Arem, B., & Van Wee, B. (2017). Policy and society related implications of automated driving: A review of literature and directions for future research. *Journal of Intelligent Transportation Systems, 21*(4), 324–348.
Nikitas, A., Avineri, E., & Parkhurst, G. (2018). Understanding the public acceptability of road pricing and the roles of older age, social norms, pro-social values and trust for urban policy-making: The case of Bristol. *Cities, 79*, 78–91.
Nikitas, A., Kougias, I., Alyavina, E., & Njoya Tchouamou, E. (2017). How can autonomous and connected vehicles, electromobility, BRT, hyperloop, shared use mobility and mobility-as-a-service shape transport futures for the context of smart cities? *Urban Science, 1*(4), 36.
Nikitas, A., Michalakopoulou, K., Njoya, E. T., & Karampatzakis, D. (2020). Artificial intelligence, transport and the smart city: Definitions and dimensions of a new mobility era. *Sustainability, 12*(7), 2789.
Nikitas, A., Njoya, E. T., & Dani, S. (2019). Examining the myths of connected and autonomous vehicles: Analysing the pathway to a driverless mobility paradigm. *International Journal of Automotive Technology and Management, 19*(1–2), 10–30.
Nikitas, A., Wang, J. Y., & Knamiller, C. (2019). Exploring parental perceptions about school travel and walking school buses: A thematic analysis approach. *Transportation Research Part A: Policy and Practice, 124*, 468–487.
Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1). 1609406917733847.
Nunes, A., Reimer, B., & Coughlin, J. F. (2018). People must retain control of autonomous vehicles. *Nature, 556*, 169–217.
Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128–147.
Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center, 26*, 311–327.
Olufowobi, H., & Bloom, G. (2019). Connected cars: Automotive cybersecurity and privacy for smart cities. In *Smart cities cybersecurity and privacy* (pp. 227–240). Elsevier.
Oppenheim, C. (1997). Managers' use and handling of information. *International Journal of Information Management, 17*(4), 239–248.
Palmeiro, A. R., van der Kint, S., Vissers, L., Farah, H., de Winter, J. C., & Hagenzieker, M. (2018). Interaction between pedestrians and automated vehicles: A Wizard of Oz experiment. *Transportation Research Part F: Traffic Psychology and Behaviour, 58*, 1005–1020.
Papadoulis, A., Quddus, M., & Imprialou, M. (2019). Evaluating the safety impact of connected and autonomous vehicles on motorways. *Accident Analysis & Prevention, 124*, 12–22.
Papoutsi, C., Reed, J. E., Marston, C., Lewis, R., Majeed, A., & Bell, D. (2015). Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: Results from a mixed methods study. *BMC Medical Informatics and Decision Making, 15*(1), 86.
Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems, 18*(11), 2898–2915.
Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*.
Pettersson, I., & Karlsson, I. M. (2015). Setting the stage for autonomous cars: A pilot study of future autonomous driving experiences. *IET Intelligent Transport Systems, 9*(7), 694–701.
Regan, M., Cunningham, M., Dixit, V., Horberry, T., Bender, A., Weeratunga, K., & Hassan, A. (2017). Preliminary findings from the first Australian national survey of public opinion about automated and driverless vehicles. Australia and New Zealand Driverless Vehicle Initiative: Sydney, Australia.
Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies, 24*(1), 231–249.
Rios-Torres, J., & Malikopoulos, A. A. (2016). A survey on the coordination of connected and automated vehicles at intersections and merging at highway on-ramps. *IEEE Transactions on Intelligent Transportation Systems, 18*(5), 1066–1077.
Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review, 34*(1), 99–110.
Rosner, G., & Kenneally, E. (2018). Clearly opaque: Privacy risks of the internet of things. *Rosner, Gilad and Kenneally, Erin, Clearly Opaque: Privacy Risks of the Internet of Things (May 1, 2018). IoT Privacy Forum*.
Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1–6). IEEE.
Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. WW Norton & Company.
Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice, 124*, 523–536.
Siegrist, M., & Cvetkovich, G. (2000). Perception of hazards: The role of social trust and knowledge. *Risk Analysis, 20*(5), 713–720.
Song, H., Fink, G., & Jeschke, S. (2017). *Security and privacy in cyber-physical systems*. Wiley-IEEE Press.
Stanley, A. J., & Clipsham, P. S. (1997). Information overload-myth or reality? IEE Colloquium on IT Strategies for Information Overload.
Steinfeld, N. (2016). "I agree to the terms and conditions" (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior, 55*, 992–1000.
Strand, N., Nilsson, J., Karlsson, I. M., & Nilsson, L. (2014). Semi-automated versus highly automated driving in critical situations caused by automation failures. *Transportation Research Part F: Traffic Psychology and Behaviour, 27*, 218–228.

Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews, 39*(1), 103–128.
Taiebat, M., Stolper, S., & Xu, M. (2019). Forecasting the impact of connected and automated vehicles on energy use: A microeconomic study of induced travel and energy rebound. *Applied Energy, 247*, 297–308.
Talebpour, A., & Mahmassani, H. S. (2016). Influence of connected and autonomous vehicles on traffic flow stability and throughput. *Transportation Research Part C: Emerging Technologies, 71*, 143–163.
Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), *Rewired: cybersecurity governance* (pp. 37–56).
Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems, 98*, 660–671.
Tennant, C., Stares, S., & Howard, S. (2019). Public discomfort at the prospect of autonomous vehicles: Building on previous surveys to measure attitudes in 11 countries. *Transportation Research Part F: Traffic Psychology and Behaviour, 64*, 98–118.
Thomopoulos, N., & Nikitas, A. (2019). Smart urban mobility futures: Editorial for special issue. *International Journal of Automotive Technology and Management, 19*(1-2), 1–9.
Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268.
Vahidi, A., & Sciarretta, A. (2018). Energy saving potentials of connected and automated vehicles. *Transportation Research Part C: Emerging Technologies, 95*, 822–843.
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.
Wadud, Z., MacKenzie, D., & Leiby, P. (2016). Help or hindrance? The travel, energy and carbon impacts of highly automated vehicles. *Transportation Research Part A: Policy and Practice, 86*, 1–18.
Waytz, A., Heafner, J., & Epley, N. (2014). The mind in the machine: Anthropomorphism increases trust in an autonomous vehicle. *Journal of Experimental Social Psychology, 52*, 113–117.
Williams, R. (2004). *Television: Technology and cultural form*. Routledge.
Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication, 800*(50), 1–39.
Ye, L., & Yamamoto, T. (2019). Evaluating the impact of connected and autonomous vehicles on traffic safety. *Physica A: Statistical Mechanics and its Applications, 526*, 121009.
Zhang, Y., Guo, K., LeBlanc, R. E., Loh, D., Schwartz, G. J., & Yu, Y. H. (2007). Increasing dietary leucine intake reduces diet-induced obesity and improves glucose and cholesterol metabolism in mice via multimechanisms. *Diabetes, 56*(6), 1647–1654.
Zhang, T., Tao, D., Qu, X., Zhang, X., Zeng, J., Zhu, H., & Zhu, H. (2020). Automated vehicle acceptance in China: Social influence and initial trust are key determinants. *Transportation Research Part C: Emerging Technologies, 112*, 220–233.