Privacy and Trust in the Internet of Vehicles

Efstathios Zavvos, Enrico H. Gerding, Vahid Yazdanpanah, Carsten Maple, Sebastian Stein, m.c. schraefel

***Abstract*—The Internet of Vehicles aims to fundamentally improve transportation by connecting vehicles, drivers, passengers, and service providers together. Several new services such as parking space identification, platooning and intersection control—to name just a few—are expected to improve traffic congestion, reduce pollution, and improve the efficiency, safety and logistics of transportation. Proposed end-user services, however, make extensive use of private information with little consideration for the impact on users and third parties (those individuals whose information is indirectly involved). This article provides the first comprehensive overview of privacy and trust issues in the Internet of Vehicles at the service level. Various concerns over privacy are formalised into four basic categories: privacy of personal information, trust, consent to provide information, and multi-party privacy. To help analyse services and to facilitate future research, the main relevant end-user services are taxonomised according to voluntary and involuntary information they require and produce. Finally, this work identifies several open research problems and highlights general approaches to address them. These especially relate to measuring the trade-off between privacy and service functionality, automated consent negotiation, trust towards the IoV and its individual services, and identifying and resolving multi-party privacy conflicts.**

***Index Terms*—Privacy, Trust, Internet of Vehicles, IoV, IoT, Connected Vehicles.**

I. Introduction

THE Internet of Vehicles (IoV) is an emerging field which is generally viewed as an extension of the Internet of Things (IoT) [1]. The latter is a global network that connects smart devices with each other. These devices feature embedded hardware and software that allows them to sense the environment and exchange information, and potentially act upon that information. When these devices include vehicles, this constitutes the IoV, with applications in *Intelligent Transportation*, *Autonomous Logistics*, and *Smart Cities* [2]. The IoV can facilitate services which are likely to change transportation drastically through shared knowledge, potentially addressing a number of issues (e.g. traffic and accident reduction). Compared to traditional Intelligent Transportation Systems (ITSs), the IoV puts extra emphasis on information interaction among entities [3]. In the IoV, vehicles are able to communicate extensively using vehicle-to-vehicle (V2V), vehicle-to-road (V2R), vehicle-to-human (V2H), vehicle-to-infrastructure (V2I) and vehicle-to-sensor (V2S) connectivity by employing various wireless communication technologies [4]. Apart from these, human-to-human (H2H) interactions through the IoV—and the human component in general—become increasingly important as services evolve.

Of course, services should focus on improving physical safety, convenience, and the cost of transportation [4]–[6]. The highly distributed nature of the IoV, however, also demands that services need to be aware of—and capable of embedding—privacy concerns. At the same time, privacy preservation is in conflict with the usability of information [7]. A *human-centred* perspective will ensure the safe delivery of services *while protecting the privacy of personal information* [8]. Thus we are focusing on the people using the services—whether of the vehicles themselves or the services hosted within the context of the vehicle. Setting practical benefits aside, privacy-awareness can further help users who are reluctant to share information trust the IoV and its services.

Although security, privacy, and trust at a vehicle network level have been explored to some extent in [9]–[12], privacy and trust at the service level remain nebulous. Proposed IoV services from the literature (see Section IV) utilise personal information (e.g. location, behavioural patterns, videos), which may additionally include involuntary information about third parties (e.g. images of pedestrians or private properties). Such improvident information sharing can lead to breaches in users' and non-users' privacy. Furthermore, access to information through the IoV raises additional concerns, such as whether the IoV can be used as a means to monitor people's activities. Privacy, however, can be a convoluted issue, because minimising information exchange can have negative impact on services and trust in some cases, making it difficult to demonstrate that service providers—and the IoV—are trustworthy.

Against this background, this work is the first to provide a comprehensive overview of privacy concerns at the level of *end-user services* in the IoV. We group these into four categories, namely privacy of personal information, trust, consent to provide information, and multi-party privacy. Other privacy issues, e.g. protecting data from unauthorised access, are related but outside the scope of this work. To discuss these concerns, we make the following contributions. First, we present a taxonomy of IoV services with regard to the privacy-sensitive information they involve. The Organisation for Economic Cooperation and Development (OECD) distinguishes between information based on its origin [13]. Accordingly, we document information provided to the service voluntarily (such as location, destination and images), and involuntary

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) through the Trustworthy Autonomous Systems Hub (EP/V00784X/1), the platform grant entitled "AutoTrust: Designing a Human-Centred Trusted, Secure, Intelligent and Usable Internet of Vehicles" (EP/R029563/1), and a Turing AI Fellowship (EP/V022067/1).

Efstathios Zavvos was with the Agents, Interaction and Complexity (AIC) group at the University of Southampton, United Kingdom during this research, and is currently with VLTN BV.

Enrico H. Gerding, Vahid Yazdanpanah, Sebastian Stein and m.c. schraefel are with the Agents, Interaction and Complexity (AIC) group at the University of Southampton, United Kingdom.

Carsten Maple is with the Warwick Manufacturing Group (WMG), The University of Warwick, United Kingdom.

information which others can obtain through observation or inference. Following this, we identify the major research challenges regarding privacy and trust in the Internet of Vehicles, present open problems and discuss potential solutions.

In the remainder of this paper, Section II provides a high-level analysis of fundamental IoV concepts. In Section III, privacy concerns in the IoV are formalised. Then, Section IV documents IoV services according to the personal information they involve, and discusses services extensively. Next, Section V discusses the research challenges on privacy and trust in the IoV explicitly, together with potential solutions. Finally, Section VI summarises the findings and highlights future steps.

II. Background

Early work on the IoV focuses on communication constraints that the flux in the topology of vehicle-to-anything (V2X) communications imposes. Hence, it is mainly concerned with Vehicular Ad-hoc NETworks (VANETs) (see [2]–[6], [14], [15]) and routing protocols (see [3], [5], [14]). In short, VANETs achieve Peer-to-Peer (P2P) communication by turning every participating vehicle into a router that helps forward messages. Nodes in VANETs self organise, but this imposes inherent limitations. For example, there is no cooperation among nodes in VANETs and this can make it difficult to integrate many computing paradigms which advanced IoV services require [15]. However, transitioning from VANETs to the IoV is not straightforward. Various architectures have been proposed for the IoV (e.g. see [16]). For example, [4] note that a vehicle cloud can help address the IoV's global character, whereas [17] argue that fog computing can solve the latency problems associated with cloud computing, and to instil the required location awareness. Recent research thus considers both clouds (e.g. [18] and [19]), and decentralised fog/edge paradigms (e.g. [20], [21], and [15]). Fog computing pushes intelligence towards the local area network, processing data in fog nodes. Edge computing pushes intelligence, processing, and communication further away from the cloud towards the edge devices connected to fog nodes (e.g. vehicles, phones) [17]. Furthermore, [21]–[23] consider social relationships in the IoV (SIoV), and [24] probes further into cognition and context awareness. Thus, achieving advanced services entails an array of challenges, which span across hardware specifications, communication protocols and network architecture, handling big data, standardisation, security and privacy, and service models among others [2], [3], [5], [14], [25]. Of these, this work is concerned with user privacy as well as with trust.

An in-depth analysis of architecture is beyond the scope of this work, but a short summary will follow to help understand how services build upon IoV infrastructure. Fundamental layers are summarised in Table I. In the IoT, [26] introduced the perception layer, the network layer and the application layer. Early IoV archetypes use a similar architecture and recent examples add several layers on top assuming TCP/IP networking (e.g. [18]–[21], [24]). It is argued, however, in [27] that the TCP/IP protocol is not sufficiently mobile for the IoV. Based on the concept of Content-Centric Networking, nodes express interests and data is communicated according to interest labels instead of IPs. Interestingly this is found to improve performance compared to using the TCP/IP protocol.

TABLE I
Fundamental IoV layers and components

IoV Layer	Components
Perception	All the sensors and hardware necessary to perceive the road and objects, establish vehicle position and so on. E.g. RADAR, LIDAR, temperature sensor etc.
Network	Hardware infrastructure, ad-hoc networks and communication protocols. E.g. LTE, WiFi, DSRC, RFID, On-Board Units (OBUs), Application Units (AUs), Road-Side Units (RSUs) [3], [5], [6], [14]
Application	Collection of tools needed for information storage, analysis and decision-making, as well as the infrastructure needed to accommodate them.

In short, built on top of the perception layer, the network layer accommodates the different modes of communication (V2V, V2I, etc.). Within the vehicle, an On-Board Unit (OBU) communicates information to other entities in the IoV, and an Application Unit (AU) provides services and distributes orders and information using the OBU. Outside the vehicle, RoadSide Units (RSUs) are fixed along the road to preserve coverage and connectivity to all vehicles. The application layer is a collection of tools and infrastructure for information storage/analysis and decision-making built on top of the network layer. Taking advantage of the ample sensory information and networking capabilities, various services for end-users have been proposed for the IoV. Currently, there are no standards to be used across services; each approach considers different technologies and service concepts or models. However, it is generally agreed that the IoV aims to address major societal needs: (1) improving the vehicles' and passengers' safety, and (2) improving the convenience and cost of transportation. For example, [5] distinguish between safety services and user applications (e.g. value-added services), whereas [14] identify safety (e.g. collision avoidance), transport efficiency (e.g. real-time traffic monitoring), and infotainment (e.g. gas station information). In [2], services are classified into safe driving, traffic control, convenience, infotainment and others.

However, these classifications offer little insight for discussing privacy concerns in the IoV, because in practice services can be very complicated (see Section IV). To some extent this is due to the complexity of individual services, which often consist of different use cases, and it is often difficult to disentangle these. To a larger degree, however, it is simply because privacy is a dismissed aspect in most approaches. Hence, to enable a robust analysis of challenges regarding user privacy, this work provides a novel classification of proposed services (see Section IV), as well as novel insights into privacy-specific challenges in end-user services (Section V).

On the issue of trust, this is especially prominent when we consider the social aspect of the IoV (SIoV). As [22] point out, the SIoV focuses on the social interaction among vehicles and among drivers. A similar concept for the IoT, SIoT, has been identified in [26] as the convergence of the IoT and social networks. In this view, every object can look for the desired services using its social relationships, querying its friends and the friends of friends [28]. In the relationship model presented in [21], relationships may not be equally lasting or important. There are de-facto long-term relationships, and short-term relationships that can evolve into long-term ones, with [29] presenting a similar view. Thus, it is important to select the right friends to achieve a satisfactory level of service in the SIoV. However, the changing network topology, constant linkage interruption and unknown network size in the SIoV make node detection difficult, and trust relationship construction very challenging [30]. This exploitation of social relationships can entail several privacy concerns, which [31] explain thoroughly. This topic encompasses the issues of privacy and trust among parties in the IoV (e.g. revealing friendly relationships, revealing personal information to friends), and sometimes results in a trade-off between privacy and trust. Specifically, although more privacy can improve trust in the IoV as a concept, it can hinder trust among parties in certain services. These are discussed further in Section III-B, Sections IV-F, IV-G in the context of vehicle platooning and intelligent intersections respectively. Challenges and solutions for establishing trust are then discussed in Section V-C.

Finally, some believe that components of the IoV need to exhibit context awareness. For example, [24] propose a model for the Cognitive IoV which utilises hierarchical cognitive engines and joint analysis to enhance decision-making and exploit the market potential of the IoV. For all its potential benefits, however, this entails several concerns with regard to the users' privacy. Related to this, Section IV-H discusses that a variety of 'smarter' applications are directed at monitoring and profiling individuals. Furthermore, enhanced intelligence generally requires more information and, hence, less privacy, but the benefits for many services remain unclear. This issue is discussed in more detail in Sections IV-D, IV-G and V-B.

III. Concerns about Privacy and Trust in the IoV

To realise the envisioned IoV services, various types of information are necessary, including potentially sensitive information such as the location of a vehicle or its destination. It is not difficult to imagine that privacy is intertwined with security when communication networks are considered, and it is a well-established consensus that the IoV will be very vulnerable to a multitude of attacks (e.g. [4], [10], [11], [17], [32]–[34]). Security and privacy are vast topics, and this paper will focus explicitly on privacy in end-user services.

There are a wide range of privacy issues in the IoV which are likely to proliferate due to the IoV's large scale, and due to the need for many services to operate at short time-scales. Existing work, such as [31], categorises concerns according to data types and the kind of privacy that is breached (e.g. privacy of images vs. privacy of behaviour), or focuses on a specific data type such as location data [35]. Whereas our work will also look into data types in the next section, data types are not the only concern and this work considers privacy issues in a more holistic manner. In particular, we identify four major privacy concerns (see also Table II); personal information privacy, multi-party privacy, trust, and consent. Such a categorisation helps put the discussion on privacy issues in the IoV into perspective. Each of these concerns—if left unaddressed—can harm the credibility of the IoV severely. A more in-depth discussion now follows.

TABLE II
A summary of privacy and trust concerns in the IoV. Personal information privacy and multi-party privacy are discussed in Section III-A, and trust and consent to share information are discussed in Section III-B

Concern	Summary
Personal Information Privacy	Users will need to share personal information. The systematic collection and storage of information poses risks for users, who may become vulnerable to attacks and exploitation. Services should use the minimal information necessary, but this may harm service quality.
Multi-party Privacy	There is a significant concern that the privacy of third parties (not users of the service) can be breached with the IoV, to a greater extent than this is possible with typical social networks. Monitoring peoples' activities through the IoV can impact trust in the IoV severely.
Trust	Trust has many facets in the IoV. Importantly, users need to trust each other and providers, and the IoV itself. Lack of trust can lead to reluctance in sharing information and using services, and can render the IoV undesirable.
Consent to Share Information	Users should consent for their information to be used, but this is difficult to scale for the IoV. Privacy trade-offs are often unclear and constant consent management in real-time can be obtrusive in the IoV.

A. *Privacy in the IoV*

Providers of end-user services in the IoV need to obtain and process enormous amounts of data [36]. The protection of personal information, at the same time, is a legal requirement in the EU with the General Data Protection Regulation (GDPR) [37], and protecting personal data is emphasised as increasingly important [38]. From the discussion in Section II, it follows that users may need to reveal personal information to service providers or other end-users. One could argue that this is no different from using other Internet services. However, IoV services may collect much more fine-grained data such as route, video feeds, emotional state, and more (see Section IV) in a more continuous manner. The systematic, large-scale collection of information may make exploiting personal information easier and more lucrative, and attackers may find the IoV particularly attractive for launching attacks targeted towards individuals [39], [40]. Furthermore, multiple malware attacks have been performed on various critical vehicle systems including braking systems [40]–[42], key-less entry systems [43], and alert messaging systems [44].

Regarding sharing personal information, [10] stress that the large number and diversity of participating parties—such as vehicle and hardware manufacturers, consumers, service providers, certificate authorities—makes aligning their interests difficult. Furthermore, more security usually means less privacy, thereby drivers may be unwilling to give up their privacy for some perceived security *and* have to worry about their security at the same time. Users may also resist the IoV if they believe they are being monitored. Indeed, our review of proposed services for the IoV in Section IV shows that consumers may have good reasons to be reluctant. Ideally, services should use the least amount of information necessary to perform the task and/or provide the service effectively, which is a crucial requirement of the GDPR [35]. This is understood in principle, but is very difficult to quantify and communicate to the user, and new approaches are necessary for data-centric privacy in the IoV [1].

A further, pervasive, issue with privacy in the IoV is multi-party privacy. This refers to the privacy of individuals who are not the requesting party of the service and may not even be IoV users at all. As [31] highlight, the fact that users can, knowingly or even unknowingly, share data on other users in the IoV, is a serious concern. In general, the excessive exchange of personal information can result in user privacy breaches. However, it is also possible for personal information of non-users to be revealed or inferred through the interaction among users and/or service providers, without the opportunity to consent. For example, [45] find that many approaches using AI in AUtonomous Vehicles (AUVs)—those vehicles which can operate without intervention by the driver—rely on image processing to train neural networks. The exchange of video recordings per request or images for identifying empty parking spaces may also contain information that breaches the privacy of non-users.

Therefore, we define a "*multi-party privacy conflict*" as the sharing of data from IoV participants that includes information pertaining to other users or non-users. Apart from privacy and consent, multi-party privacy also permeates trust. Even when there are no direct repercussions for sharing personal information, having the impression that the IoV may monitor or access people's activities can render the IoV undesired, and this impression can be reinforced with actual multi-party privacy conflicts. We recognise this as one of the most serious privacy issues in the IoV, since it can lead both end-users and wider society to perceive the IoV as untrustworthy.

B. Trust in the IoV

Trust is an important concern in the IoV with numerous mentions in the literature (e.g. [31], [39], [46], [47]). On-demand services will likely see unprecedented usage in the IoV. Building trustworthy IoV systems, therefore, can be highly complex due to the large scale of the IoV and the sensitive information many services will require. As discussed in Section II, trust is multifaceted and may include trust among users (e.g. [46]), trust between users and service providers [17], [32], trust between network nodes when propagating information automatically [17], trust during fog orchestration [17], finding trustworthy edge devices to offload computations to [48], as well as the credibility of the IoV concept itself.

Users may avoid utilising the full spectrum of services, focusing on services from trustworthy providers or services which other trusted parties use (e.g. family). Moreover, people may distrust the IoV altogether if they anticipate the risk that their personal information can be exploited. This can remove any incentives users may have to provide the required information for the effective performance of the IoV. Meanwhile, evaluating trustworthiness in the IoV is highly challenging because it is decentralised [16]. Trust must be handled in real time but networks may be congested in peak hours and reaction time in the IoV is limited. Thus, (1) minimising obscurity in service models, (2) making the intent of information usage clear and legally binding for providers, and (3) employing privacy-by-design concepts could help protect the privacy of the user, facilitating the process of building trust in the IoV.

In addition to data that is collected willingly for specific purposes, data in the IoV can often be collected when not required and can potentially be stored and reused without the user's consent [31]. Therefore, a significant related issue is consent to share information. Among several obligations the GDPR imposes on software operators and service providers, a key obligation is user consent [33]. The complex granularity in the IoV together with the fleeting character of services, however, obfuscate the matter of making informed consensual decisions. This may even result in exploitation of personal information (e.g. payment info, images, location history, driving habits) and activity monitoring *even with the user's consent*, and may make it easier to inflict physical or psychological harm.

Today, social networks and mobile applications constantly refine privacy control features. However, privacy settings still lack the ability to fine-tune permissions in some cases [49]. Consumers often lack enough information to make privacy-sensitive decisions, and—even with sufficient information—they are likely to trade off long-term privacy for short-term benefits [50]. It is argued further in [50] that users consent to personal data sharing by accepting opaque and inflexible policies which are rarely read, indicating that constant consent requests may be inefficient and obtrusive. These are disconcerting findings as we expect consent-based information sharing to be the core of the IoV design and deployment.

IV. Personal Information in IoV Services

To better understand where privacy concerns arise, this section documents services in the context of the IoV more systematically, based on types of information services involve. Services are then discussed in terms of privacy concerns. In general, we observe that advanced IoV services use more information, and rudimentary services use less. For example, [51] propose a smart helmet for motorcyclists that shows driving information such as speed and navigation information and sends an SMS in case of collision. This requires little personal information, but also does little to take advantage of the IoV's potential. It will become clear in this section that there is a trade-off between privacy and service quality, something also supported by [7]. Thus, it will also be discussed whether the same or a similar service can be acquired using less information.

Broadly, we have identified seven main categories of IoV services. These include: event-driven services, parking space identification, Mobile CrowdSensing (MCS), social networking, vehicle platooning, intelligent intersections, and services that are proposed as monitoring applications. Table IV provides an overview of information usage in IoV services. As shown, services in the IoV generally require some form of unique identification and GPS information. Many services additionally require route information and/or multimedia feeds in the form of video, images or sound recordings. Moreover, for most services, it is possible to determine involuntary information on users or third parties, especially information which can identify them and place them at certain locations.

TABLE III
INFORMATION GROUPS DOCUMENTED IN THIS STUDY

Group	Explanation
ID	The information or ability to identify a vehicle, user, or third party uniquely (e.g. name, licence plate, mobile ID, and service account).
GPS	Information that can be acquired through a GPS device (geolocation, velocity, direction, and timestamp).
Route	Information on the vehicle's origin, destination, and the path travelled/to-travel.
Multimedia feeds	Video, image, or sound information that can be acquired either through on-board sensors or other devices such as mobile phones.
Profile	Any information that can be used to profile a person. This can include behavioural patterns, driving habits, health records, and emotional state.
Interests & Relationships	Information that can reveal a person's interests (excluding destination and route) and/or social relationships.
Other	Information that is acquired from other sensors that do not fall in the previous categories (e.g. RADAR, LIDAR, ultrasonic).

A. Documenting Information in Services

Information in IoV services may include various types. We group information into seven categories which can compromise privacy. These follow closely information types used in other work [7], [31]. To understand where privacy conflicts can arise, information has been grouped according to common uses and in categories that, in combination, can be dangerous to the user and can be seen in Table III.

Moreover, in Table IV, for each service two items are documented in each information category of Table III. The first is whether the user is required to provide the information voluntarily, indicated with a (●), and essentially refers to 'provided data' as per the OECD's classification [13]. The second is whether it is possible for information to be observed, inferred or obtained in any way, where the subject may not realise the information is being produced/recorded. We consider this involuntary information, indicated with a (○), aggregating together OECD's 'observed data', some of 'derived data', and 'inferred data'. These data may concern a vehicle's driver or passengers, or third parties who may even be unaware of the IoV. The provided list does not serve to exhaustively examine proposed services in the IoV but rather to identify and evaluate more general service categories in terms of privacy.

B. Event-driven Services

In [54], the concept of event-driven services is introduced. For example, traffic lights can be switched to red automatically before an ambulance passes through an intersection. The logic is that an ambulance can broadcast event information to fog nodes near its travelling route. Then, fog nodes like cameras receive events and can generate an additional event representing the ambulance observation at intervals. Finally, cameras near crossroads can identify the ambulance via image processing, and an event processing agent can switch the light to red. Event-driven services can be problematic, not only with respect to the privacy of personal information, but also regarding the reliability of services. The authors in [54] recognise that events generated by vehicles can be uncertain, which will affect service quality. In turn, ensuring a certain level of quality requires a large amount of information. Furthermore, event-driven image processing in every intersection is disconcerting with regard to potential uses and multi-party privacy.

C. Parking Space Identification

In [52], the authors propose a real-time parking space monitoring and guiding system where the user sends a request to park coupled with the GPS information. Then, the service allocates nearby vehicles the task of photographing parking spaces. Images are tagged with location, and the service analyses and stores them. Upon finding a vacant space, the driver is guided towards it. It is arguable that stored images may contain information on parked vehicles and their identification, together with their location and time, and may additionally include information on pedestrians, which can breach multi-party privacy and the privacy of personal information. Systematically storing such information may provide incentive for hacking such a system e.g. to monitor a particular area.

Other approaches attempt to minimise the use of personal information. However, we observe that such methods may hamper the quality of parking space identification. For example, [53] attempt to identify empty parking spaces by using ultrasonic rangefinders instead of imaging. This is much less invasive, but vehicles that carry the sensors still communicate location data to the server. The authors note that an accurate GPS may be more effective in measuring the size of the space, because ultrasonic rangefinders are susceptible to echoes coming from an angle. This highlights that there may be a trade-off between privacy and effectiveness of the service. Furthermore, we note that, while identification is undoubtedly useful, there are alternatives that do not require any information at all, such as parking lots whose availability drivers can already see today. Although this is not as convenient, it could provide inspiration for developing solutions that require less personal data.

D. Mobile CrowdSensing

The mobility in the IoV has inspired services that involve some form of participatory Mobile CrowdSensing (MCS), where users contribute sensory data to help infer information on matters of common interest. It is straightforward to see how such solutions could be deployed under the control of an academic institution, but when it comes to fully deployed commercial applications, these approaches require personal information on several levels. MCS, therefore, yet suffers from the common issue that the incentive for users to provide information is unclear. Even in cases where the user decides

TABLE IV
AMONG THE LIST OF SURVEYED PUBLICATIONS (COLUMN 1), WE IDENTIFIED IF THEIR PROPOSED IOV SERVICES EXPLOIT PERSONAL INFORMATION. FOR EACH OF THE INFORMATION CATEGORIES IDENTIFIED IN TABLE III, WE DOCUMENT WHETHER INFORMATION PERTAINING TO EACH CATEGORY IS PROVIDED BY THE USER VOLUNTARILY (●), INVOLUNTARILY (○), OR BOTH (○ ●).

	Information						
Publication	ID	GPS	Route	Multimedia feeds	Profile	Interests/Relationships	Other
Parking finder [52]	○ ●	●	○	●			
Parking finder [53]	●	●	○				●
Event-driven services [54]	○ ●	●	○ ●	●			
Traffic monitoring [55]	●	●	●				
Traffic monitoring [56]	●	●	●	●			●
Sensing tasks [57], [58]	●	●	○ ●	●			●
Navigation [59]	●	●	●				●
Cooperative routing [60]	○	●	●				
Intention-aware routing [61]	●		○ ●				●
Cooperative charging [62]	●	●	●				●
Car-sharing rentals [63]	○ ●	○ ●	○ ●				
Safety warnings [21]	○	○ ●	○ ●		●		
Automatic emergency response [19], [21]	○ ●	●		●	○		●
Voice chat [64]	○ ●	●	○ ●	●	●		
Vocal warnings [65] (Social navigation)	○ ●	○ ●	○ ●	●			
Location-based queries [20]	○ ●	○	○	●			
Proactive monitoring [66]	○ ●	○ ●	○ ●	●	○		
Driver assistance [24]	●	●	○	●	○	○ ●	●
Driver assistance [67]	●					○	●
Pedestrian identification [24]	○ ●	○ ●		●	○	○	
Platooning [68]–[72]	○ ●	●	○	●			●
Intelligent Intersection [73]–[81]	●	●	○		●		
Intelligent Traffic Light [82]	●	●	○		○ ●	●	

to use such a service, the privacy of systematically collected personal information is a significant concern.

A system where users can upload the desired destination in order to acquire traffic information is presented in [55]. An incentive mechanism is usually offered for provision of data such as mobile id, speed, location, direction, from which traffic conditions can be inferred. The authors, however do not provide further information on the mechanism. In [56], smartphones drivers carry are used to monitor road and traffic conditions. Specifically, the accelerometer, microphone, GSM radio, and GPS help detect bumps and potholes as well as braking and honking. In [59], the authors present a system for drivers to log events of interest using their phones. The data is collected and processed in a server, where human input is aggregated and the information is disseminated based on the driver's location. Then, it is used to provide up-to-date, congestion-free paths in real time. For example, the path can dynamically adjust due to a logged accident on the road.

These solutions do not address incentives to provide information explicitly and require user participation to operate effectively. However, according to [55] it is natural for users to be reluctant in providing information. In the case of [55], [56], it can be argued that the acquisition of the service itself is an incentive, and [59] make a stronger case for this with a system that provides a more up-to-date route. Providers could integrate privacy-by-design methods into their service, to enhance the users' trust in the provider, making the incentive for users to participate more clear. For example, in [83] Virtual Trip Lines (VTLs) are used, which associate the traffic information transmitted with virtual landmarks, rather than with the location and ID of the vehicle. This is further employed in a proof-of-concept by [84]. The VTLs consist of two GPS coordinates which draw a virtual line across a roadway of interest. Phones have a list of VTLs and upon crossing one, they can send an update with anonymised position, speed and direction. A particularly interesting finding is that only 2%-3% of mobile phones in the driver population are necessary in order to obtain reliable traffic information.

An additional risk in the collection of traffic data is vehicle trajectory reconstruction (e.g. [85]). Vehicle trajectories are of high statistical value for many transportation applications, such as designing public transit systems, environmental and safety assessments, and modelling human behaviour [86]. Nevertheless, when paired with named data collection and storage it can be problematic for the privacy of personal information. Although [84] used VTLs to anonymise data collection, they tried to minimise the possibility to reconstruct trajectories by allowing mobile phones to ignore some VTLs, and the server to ignore data points from neighbouring VTLs.

A method to select vehicles for specific sensing tasks is shown in [57]. Task publishers announce multiple sensing tasks with a reward budget, and a coordinator assigns these to appropriate participants, with applicability in more general settings. Participants are constrained by the road topology and information needs to be collected continuously while they are moving. The coordinator, therefore, needs to assign tasks according to vehicle routes in order to improve coverage. It is evident that participants need to share with the coordinator private information regarding their route, trajectory and location. An incentive mechanism is assumed to exist, without further information. In [58], the authors propose a system to visualise data from vehicle sensors through a central portal that collects and analyses sensory data from vehicles. The portal provides an API for developers to utilise the data, or to query vehicles for data. Collected data is characterised by sensor name and ID and the vehicle ID, and is organised in terms of traces, that is sets of sensor readings collected during a particular drive. It can then be visualised according to these traces. This architecture can be considered unaware of privacy concerns as user data can be correlated to the time and location they were obtained, as well as the car that obtained them and its route.

E. Social Networking

Under the scope of the SIoV, [60] propose cooperative vehicle routing, where drivers cooperate in reducing the individual and total travel time. This is more efficient than non-cooperative methods, but every driver knows where all other drivers might be going and via which route. A similar concept is presented in [61], where electric vehicle (EV) drivers exchange routing intentions through an intelligent transportation system (ITS), and potential queuing times at charging stations are calculated. Then, drivers decide on their routes so as to minimise their expected cost of travel. It is understandable that each vehicle must submit route information to the system.

A different concept is presented in [62], where EVs coordinate to meet and exchange charge in order to minimise total energy lost and the probability of EVs being stranded. Coordination is done by maintaining distance and path quality information about the immediate neighbourhood of a vehicle, with decreasing detail as the distance increases. To test the model, historical GPS data from taxis are used. However, it is not straightforward what incentive drivers have to give up sensitive personal information to meet people with whom they have no prior established trust. [63] propose a service where a provider owns vehicles available for sharing. The system can recommend the nearest vehicle station based on the user's location, and vehicles are assigned to multiple passengers. Although similar to ride-sharing, trust plays a significant role in this service. Specifically, we deem that it is not reasonable to assume that random people may meet to rent a vehicle jointly with no mediating party present (e.g. an Uber driver).

The above cases involve obvious risks but others involve more obscure ones. Vehicular Social Networks (VSNs) are introduced in [64] with the idea of drivers joining discussion groups along roadways. When the journey starts, the client application logs into desired groups along the way, e.g. a political discussion group, based on the driver's location. Voice messages are recorded and transmitted to the server with a timestamp and user information. In a similar manner, [65] integrate driver-provided information into a social navigation system to calculate a personalised route. Drivers share events of interest by recording voice tweets. Other drivers can hear the tweet digests and instruct their navigation device to e.g. avoid a certain route. Tweets are tagged with the vehicle's location, speed, current time, and driver ID. Such services require multiple private data to operate, entailing various privacy-related risks [7]. The fact that voice messages can be recorded and stored can also be problematic for the user's privacy. In the case of social navigation, it could be used to track a person's presence at a certain location.

F. Vehicle Platooning

A vehicle platoon consists of a leading vehicle, and other vehicles who follow the leader [69]. It is assumed that at least the leading vehicle has to be driven by a driver, whereas followers can move autonomously, but this could change with the evolution of technology [69], [72]. Vehicles can also dynamically join or leave platoons as is the case in [69]. Platooning expected to enhance safety, reduce travel costs and increase road capacity [71], [87]. In fact, [88] show that the capacity of a single highway lane can be increased by a factor of two to three, if vehicles drive in platoons of up to 10 cars. Considerable fuel saving has also already been demonstrated, which in the case of truck platoons will have a large impact on the cost of goods transportation [68], [87]. To accommodate platooning, [72] use computer vision to detect lanes and the lateral position of a vehicle, and a combination of RADAR and LIDAR for longitudinal observations. In addition, vehicles communicate with each other via IEEE 802.11p and infrared; other projects utilise a similar configuration [69]–[71], [87]. An important issue in platooning are longitudinal oscillations that may occur due to slow information propagation from the lead vehicle to the back, when only local sensors are used. To attenuate traffic shock-waves, it is thus paramount that information from all vehicles be shared among the platoon. [72] share the velocity of each vehicle, the braking signal, the position in the platoon, obstacle locations, and the position of each vehicle. In addition, it is necessary for each vehicle to be uniquely identifiable within the platoon. Similarly, [70] convey a vehicle's sensory information to the other vehicles and the data are fused to create a more complete perspective of the platoon's surroundings.

However, in relation to privacy, we identify two main issues. First, information sharing can be exploited. For example, [89] propose a system for a car to query and access sensors on other cars as if they were its own. At the same time, most literature also assumes that vehicles should be equipped with Radio-Frequency (RF) identification, and [90] present a method based on RF sensing for locating and navigating to a target of unknown location, using only RF measurements provided by a network of nodes surrounding the target (e.g. a platoon). Therefore any car in a platoon can be located if someone remotely queries its neighbours' sensors. Second, the ability to identify vehicles uniquely, and also visually, has implications. For example, it is possible for vehicles in a platoon to infer the origin, destination, and route of each other, and to monitor the activities of their passengers visually. When acquaintances use a platoon, e.g. to go to work, this may be acceptable. However, in public platoons, it raises significant concerns on the privacy of users, and it is not clear how platoon users can trust other platoon members.

G. Intelligent Intersections

Intersection efficiency and scheduling is a central topic when it comes to enhanced intelligence. In short, intelligent intersections manage traffic through the usage of appropriate coordination technology and algorithms, rather than through traffic lights and signals. This is expected to bring about better space utilisation, and delay and accident minimisation [79].

A control agent is proposed in [75], which gathers information about individual vehicles and provides the best sequence of manoeuvres to vehicles crossing the intersection, avoiding collisions by eliminating overlaps in vehicle trajectories. In [74], cars negotiate crossing the intersection through a mixture of centralised and distributed decision making, which solves a time slot reservation problem. The authors, however, state that the solution does not scale well with an increasing volume of traffic. A similar observation is made in [73], using a time-slot reservation multi-agent approach. Cars receive time slots during which they may pass the intersection, and it is of note that there is a trade-off between complexity and the size of the grid considered in the intersection. [76] solve the problem of evacuating vehicles from the intersection as soon as possible, for each sequence of arriving vehicles, using dynamic programming. To reduce complexity, they also present an ant-colony optimisation approximation which works in real time.

In [78], decisions made by each vehicle are integrated into scheduling. Vehicles are ordered according to arrival time and properties of the vehicles, and the vehicle with the highest priority is permitted to cross if its route does not conflict with those already permitted. [80] propose that vehicles in the same lane are divided into small groups and these groups are scheduled to cross an intersection through the use of a neuro-fuzzy network-based mechanism. In [77], an auction is conducted at each intersection so that travellers can self-organise using a pricing mechanism which prioritises higher-valued trips. A system agent at the same time bids benevolently at a level which guarantees a minimum service quality for those not willing to pay. A smart traffic light in [82] decides on the time intervals of red and green based on various factors, including the social characteristics of passengers. They introduce a social preference parameter to make traffic handling more just, and to reduce driver stress (e.g. late for work has higher priority). Green light time is determined by the sum of priorities for each direction of traffic. However, it is not explained why the drivers would report their true preferences.

Despite the expected benefits of intelligent intersections, there are challenges that go beyond those in [91]. Intelligent intersections necessitate rigorous communication of information that includes GPS information, and in some cases user profile information to help negotiate priority. If such data are stored or exploited, the routes of all vehicles can be inferred. At the same time, less intrusive technologies have been proposed. For example, [92] test an advisory system to notify drivers of stop sign intersections, which detects stop-sign beacons and provides an audible alarm. It was found to help reduce approaching speed, and participating drivers found it useful and unobtrusive. However, until we achieve AUVs, there may be several services to assist drivers with minimal sacrifice of privacy. Importantly, it still not clear if and under which circumstances intelligent intersections can provide significant benefits. For example, [73] find that introducing only 10% human drivers into scenarios with AUVs can render intelligent intersections as useful as traffic lights, and [81] show that communication delays can severely impact performance. Therefore, the key question is whether a trade-off in privacy is worthwhile.

H. Potential Monitoring of Individuals in IoV Services

Beyond the aforementioned services, a variety of other concepts have been proposed which may result in intensive driver profiling and/or monitoring. In [19], the authors propose automated calls to emergency services, family or friends, which include information related to the situations the vehicle has been in, including the number of passengers, direction, location, and cause of emergency. Furthermore, they propose that vehicles should communicate with parked vehicles to cooperate in finding parking places. These services can breach driver and passengers privacy, and raise concerns regarding consent. The statistical analysis of usage information such as driving behaviour, duration, and traffic rule violations is proposed in [19] to obtain personalised insurance quotes. The authors argue that this leads to reduced insurance cost in theory. However, we argue that, in practice, this leads to undesirable power asymmetries between insurers and end users. In addition, it may harm the trustworthiness of insurance firms as drivers may feel they are being monitored.

In [20], vehicles are informed of accidents via beacons. The vehicle can then request a video feed from a camera facing the accident. While it is understandable that, in emergencies, such a function could be useful, in general the concept that anyone may request video from a location of interest is very troubling. Similarly, [24] envision that driving behaviour, emotional condition, and fatigue state can be uploaded to a private cloud which can infer personalised rules about drivers. Such a function can lead to serious trust issues during the deliberation of the service (within the same vehicle) or prior to that, e.g. it may provoke racial profiling and discrimination. [24] also propose that enhanced intelligence could help identify a pedestrian target, analyse information such as height and age to predict dangerous acts of the target. In [66], data from vehicles are used for proactive urban monitoring, and authorities can search the vehicle network for witnesses or evidence. These concepts, while proposed with good intentions, may trigger several multi-party privacy conflicts and may also raise ethical concerns with regard to the social relationships such systems would encourage.

A further range of applications is presented in [21], where real-time data from vehicles can be collected based on social relationships. For example, the car holds knowledge about the driver's social contacts and uses this to build a social circle with other vehicles sharing the same interests. In addition, the vehicle keeps the fog updated by constantly synchronising data. This way, safety notifications from relationships can be received, such as for roadworks, based on their observations. Whereas the exploitation of social relationships has several advantages, it also has disadvantages. Specifically, many of the social relationships may depend on mutual interests. This could be, for example, the same workplace or having the same destination. Users may thus be able to infer personal information of their social relationships by using such services.

V. Challenges and Future Directions

The preceding sections have identified several issues and challenges with regard to privacy in IoV end-user services. It is interesting to note that, although the privacy of users and non-users, and the trust in the IoV are clearly important, consumer surveys around connected and autonomous vehicles do not highlight specific ways in which privacy could be affected. For example, a study in the UK by Autodrive and the University of Cambridge, showed mixed opinions in the general population, on whether they would use driver-less vehicles [93]. Similarly, Deloitte showed mixed results in Japan, the U.S. and Germany, with less than 50% of the participants believing connected vehicle technology will be beneficial [94]. These results were obtained while failing to explain to participants the implications of the information sharing involved, or privacy concerns concepts such as platooning introduce, which we believe is crucial to evaluate consumer trust in the IoV. Additionally, the swift and ephemeral nature of services make it difficult to design usable solutions that protect privacy and enhance trust without compromising functionality. This is expected to pose a significant hurdle for IoV services to overcome.

To provide insights into the privacy and trust issues in the IoV, and to discuss areas of interest for future research directions, this work identifies six major challenges which are summarised in Table V. These are discussed in more detail in the remainder of this section.

TABLE V
Privacy and Trust challenges in the IoV

Challenge	Summary
Standardisation	Protecting privacy is difficult because of the range of services and the lack of standardisation. There is a need for new privacy protection concepts, and for incorporating existing privacy-by-design methods.
Privacy Trade-off Analysis	There is a trade-off between privacy and functionality in many IoV services. Quantifying this and finding a balance is a challenging future direction.
Building Trust	Establishing trust is expected to be significantly challenging, given the ad-hoc nature of the IoV, and large-scale information propagation. Moreover, sometimes there is a trade-off between privacy and trust. Working towards improving both privacy and trust at the same time is a worthwhile topic.
Meaningful Consent	Consent negotiation is obtrusive, especially when consent needs to be constantly provided in real-time. Leaps need to be made before automated consent negotiation is effective and meaningful in the IoV.
Incentives Engineering	The incentives for the user to provide information are unclear in many services. Incentive mechanisms are taken for granted in most services and it is necessary explore them more systematically in the IoV.
Multi-party Privacy Analysis	Multi-party privacy in the IoV needs comprehensive research. The opportunities for breaching the privacy of third parties are many, while the opportunities to identify and defend against breaches are few. This can have serious consequences for the safety of individuals and can harm trust in the IoV thoroughly.

A. User Privacy and Privacy-by-Design

We expect user privacy protection to be challenging, and this may have a significant impact on the adoption of IoV related technologies, as well as on the welfare of users themselves. For instance, the cognitive IoV (Section II) is envisioned to utilise various types of personal information such as facial expressions and emotional state. However, to preserve the privacy of users and, at the same time, to enhance intelligence does not necessarily mean that every application in the IoV has to be over-engineered. For example, [67] propose a method that can be effective in driver fatigue detection by recording only ECG data obtained from the driver. Additionally, [95] review a multitude of driver fatigue detection systems that record only one kind of information such as blood pressure or sleep patterns. Whereas such information could be exploited, e.g. to infer users' reaction to advertisements, they are mindful of privacy than the thorough driver profiling proposed in [24].

TABLE VI
An overview of useful privacy-by-design methods for the IoV

Paper	Method	Application
[23], [29]	Privacy Labels	Data privacy
[1], [33]	Blockchain methods	GDPR compliance
[83], [84]	Virtual Trip Lines	Anonymous data collection
[96]	Private Info. Retrieval	Anonymous data retrieval
[97]–[99]	Differential Privacy	Anonymous data retrieval
[100]–[103]	Group Signatures	Anonymous signatures

Due to the broad array of applications and contextual concerns, standardisation and privacy-by-design are not straightforward and these are areas open to research. Some inspirational work on privacy-by-design for the IoV is summarised in Table VI. In more detail, [23] and [29] propose dividing content according to privacy labels. An authority determines which part of a message must be public, and OBUs can only exchange public content. Private content can then only be shared by the owner of the vehicle by labelling it as protected. As [22] note, however, a key weakness is that it relies on the recipient honouring the privacy label. A further concept, compatible with privacy-by-design, is the blockchain. This was introduced with the advent of cryptocurrencies and refers to a decentralised and distributed digital record of transactions across computers, with applications in privacy protection and cryptography. In [1], the IoV is used as a case-study of the IoT, and integrating the blockchain into IoV system architecture is found to have a significant positive effect on preserving user privacy and complying with GDPR privacy regulations. A formal model is proposed in [33], for automatically verifying GDPR compliance on data processing units, and for verifying the compliance of smart devices during their design.

Privacy-by-design can be further employed per individual service, as in [84] who employed VTLs to collect anonymous traffic data. Similarly, [96] attempt to protect privacy in location-based services i.e. services which answer users' queries to points of interest using Private Information Retrieval. Authors find that replacing user location with the road the user is on reduces computational complexity and service error compared to grid-partitioning models. Further work includes differential privacy which has its roots in cryptography (discussed in detail in [97] and [98]). In short, this concept proposes that information about statistical databases can be published without disclosing the private information of database records, by introducing some amount of noise in the data. This is extended in [99] into ϵ-differential privacy, which defines the privacy loss mathematically to determine an amount of noise with similar effect as removing the individual's data from the database. A further well-defined concept are group signatures, which allow users to sign messages anonymously on behalf of a group. There are provably secure approaches [100], lattice-based approaches suited for dynamically growing populations [101], more recently extended for use in the IoT [102]. Modern schemes also include mesh signatures, which [103] adapt for use explicitly with the IoT. In this scheme, users can generate a mesh signature using their atomic signatures, without revealing the atomic signatures used.

B. Privacy and Functionality Trade-off

As we have seen in Section IV, in many cases, there is a trade-off between privacy and functionality. This is interesting not only from the users' point of view, but also for the business aspect of services. It is currently unclear whether the gain for users for certain services outweighs the sacrifices in privacy and there are no good approaches and tools to help users make informed decisions. At the same time, there are opportunities to investigate whether similar or better services exist which could utilise less information. Ideally, users who care about privacy should be able to easily compare the use of private information by similar services to make such decisions.

For example, in contrast to the more mindful VTL concept discussed in Sections IV-D and V-A, [59] propose traffic monitoring where drivers provide named sensory data and can also input events of interest along their route. This, in theory, results in more up-to-date navigation, but compromises privacy compared to the usage of VTLs. Concerning intelligent intersections, as discussed in Section IV-G, it is not yet clear whether a trade-off in privacy is beneficial in realistic scenarios. Additionally, [87] show that the closer vehicles are together in a platoon, the higher the savings on fuel. However, the closer vehicles, the lower the privacy of passengers may be (e.g. passengers are more visible to others).

Therefore, we believe that, to better incorporate privacy protection into services, future work should focus on quantifying the trade-off between the loss of privacy and service quality. In this paper we introduced a qualitative approach to help visualise the loss of privacy (see IV-A), and more quantitative methods are still an open challenge. Whereas concepts such as ϵ-differential privacy combined with efficiency metrics (e.g. simulations) can help measure the trade-off between privacy and functionality, these approaches can only be applied to limited types of services which exploit statistical databases. Considerably more work is needed before the trade-off can be quantified in a more general and meaningful manner.

C. Establishing Trust

As seen in Section IV, many services in the IoV involve large numbers of participants. To accommodate this, services may therefore need multi-hop routing, cloud/fog computing (Section II) and multiple network channels, which makes establishing trust among participants (vehicles, RSUs, providers) a significant challenge [9]. For example, [17] note that two limitations are that (1) edge devices (e.g. cars, phones) will face difficulty in identifying trusted nodes and (2) using trusted third parties is very difficult when considering only segments of the whole network. It is further noted by that, due to the large scale and number of stakeholders in the IoV, choosing who is going to be a Certificate Authority (CA) will be challenging [10] and secure key generation is expected to be very difficult [9]. On top of these, devices such as vehicles, sensors, gateways and control units will need to be updated constantly. Toward secure software updates, [47] propose a blockchain-based identity and trust management framework.

Apart from the technical aspect of establishing trust, there are significant conceptual challenges as well. Following from the discussion in Section IV-F, an obvious candidate solution to trust issues in, for example, vehicle platoons could be to use a recommendation system where a driver can search for platoons with better 'trustworthiness', similar to the work in [28]. However, this, in turn, requires users to have profiles and this could provide incentive to sacrifice some privacy to improve one's trustworthiness. An issue, thus, is that more privacy for the user may, on one hand, lead to improved trust in the IoV as a system but, on the other hand, it may compromise trust amongst users and/or service providers. A recommendation system is used in [30] as well, in the context of SIoV services. Historical access records of nodes are combined with node recommendation information in order to construct social relationships between nodes based on implicit similarities among vehicles. In addition, vehicles trajectories are used to estimate vehicle interaction time. These pose significant privacy concerns and highlight that in many cases there may be trade-offs between trust and privacy.

TABLE VII
AN OVERVIEW OF TRUST ESTABLISHMENT METHODS FOR THE IOV

Paper	Method	Application
[28]	Rater-based trustworthiness	Trust among nodes
[46]	Ratee-based trustworthiness	Trust among nodes
[39], [104]	Digital Forensics (Blockchain)	Evidence for crimes
[39]	Digital Forensics	Evidence for crimes
[48]	Blockchain methods	Trusted fog computing
[105]	Blockchain methods	Security & trust issues
[32], [106]	Trusted Authority mediation	User & Service trust
[107]	Relationship-based model	Initialising trust
[30]	Relationship-based model	Trust among nodes

Nevertheless, significant work to inspire future research has been carried out recently towards improving privacy *and* trust at the same time (see Table VII for a summary), but there are several limitations. Although these are privacy-by-design methods, we discuss them here because they focus on solidifying trust. One direction is toward digital forensics, and a relevant summary in the context of the IoT can be found in [104]. In the IoV, [39] propose creating evidence stories that are not related to particular interactions and actors using blockchain techniques. An investigator can then decide which stories to investigate, and the system is difficult to compromise. A challenge, however, is the plethora of possible evidence, data formats and distributed infrastructure. Other work focuses on trust management. Traditional rater-based models store the reputation of each node in other nodes it interacts with, but networks in the IoV are ephemeral. Ratee-based management in [46] instead stores reputation rated by others during interactions within the node itself, and a CA server ensures the authenticity and integrity of trust information. This results in faster information propagation and better transaction success rate compared to rater-based methods.

The blockchain is again used in [48], where parked vehicles compete with each other to earn income from the computation offloading service, the goal being to maximise service performance and reduce user fees. Although the blockchain (see also Section V-A) can indeed address a number of privacy and trust issues in compliance with GDPR regulations, it still suffers from security (cyber-attack) and trust issues at other levels, such as when propagating information. Several challenges with regard to the blockchain are discussed in detail in [105]. Initialising trust degrees among vehicles is difficult, and [107] propose initialising trust values based on offline social relationships and a satisfaction rating for interactions, but they do not show a mechanism to guarantee truthful ratings. It is noted that in the latter two approaches, anonymity is not guaranteed. To address anonymity, [106] and [32] propose facilitating interaction between IoV entities through a trusted authority (TA). In [106], vehicles register to a TA and authenticate with each other without knowing who the other party is. They show that this scheme can resist numerous types of attacks, while improving computing capacity and communication overhead compared to previous schemes. In [32], a similar approach facilitates privacy when a user requests a service; a cloud broker managed by the TA connects the user to a registered service, and the selection of provider is hidden for the user. Third parties cannot link intercepted messages to the vehicle or provider. However, this approach makes it difficult for providers to build their trademarks in practice, and does not leave much room for the user to choose a service provider either. Furthermore, it is not clear how the TA can handle perhaps many millions of such transactions at any given time.

D. Consent Negotiation

As discussed, privacy-by-design solutions are promising in various IoV services. However, it is understandable that this may not be possible for all applications in the IoV. Furthermore, the issues of trust and consent (raised in Section III-B) necessitate solutions that are efficient when it comes to managing privacy and supporting consent negotiation.

To address the limitations of manually managing complex privacy settings and requests to access personal data, [108] propose the use of agents to autonomously negotiate these on behalf of the user. In their model, the agent learns from interactions and the user can make further manual refinements. The authors find this can be effective in capturing the preferences of the user and in negotiating on the user's behalf, but there are several challenges open to research. For example, the evaluation in [108] was limited to only five different data types. As the authors rightly note, in reality, negotiations are expected to be much more complicated and to include many more issues at the same time, such as who the receiving party is (i.e. to build trust), for how long the data is to be retained, the purpose of the data collection, and the privacy risks involved. Capturing the preferences of these options while minimising user bother is a major challenge. Among other challenges [109] identified in automated negotiation, we emphasise the following two. First, the user needs to trust the agent enough to surrender control, but at the same time it is challenging to obtain the user's trust and to make automated negotiation widely adopted. Second, limited access to automated negotiation technology could further intensify existing social injustice, something which we extend as a future direction through all levels of life-changing automation in the IoV (e.g. driver-less vehicles).

E. Incentives for Providing Information

In Sections IV-D and IV-E we highlighted many cases where the it is not clear whether there is an incentive for users to provide personal information. Although the system or the service benefits from having the data, this does not necessarily mean the individual providing this information benefits as well. Hence, in this paper, we identify incentives as a further major challenge in the IoV. This includes incentives to provide personal information, and also incentives to use automated agents such as those in V-E, and the agent that negotiates crossing an intersection in [77] (Section IV-G). Approaches such as [55] and [57]—presented in Section IV-D—assume incentive mechanisms for users to give personal information based on the idea that the service itself is a reward.

The service itself is indeed a tangible benefit for the user. However, it is still very difficult to weigh this gain versus the information sacrificed in order to make informed decisions, and this is obtrusive for the user when it has to be done constantly. To have an incentive, the user must be able to perceive trade-offs as beneficial. For example, even if only one negotiation severely backfires for the user (e.g. user is exploited), this may be enough to lose trust in automated negotiation completely, and this effect could propagate across the user's social contacts. This is a major risk in the IoV considering the potentially very high number of such data provision negotiations likely to take place for each user.

Related to the above and also to the discussion in Sections V-B and V-C is the fact that, it is challenging for ordinary users to understand the risk of sharing information. Services like Facebook are indeed free for the user to use, but follow a business model where the user is actually the commodity the service sells to third parties like advertisers [110]. This is done by exploiting and monetising the user's data, and it is argued that users should have a right to know the value of their data [111]. Whereas there is literature on how to compute the value of data for providers (see [110] and [111]), little has been done on identifying and measuring the risks for users.

Furthermore, it is not yet clear how incentive mechanisms can be validated effectively. [108] offered real money as incentive to participants for using an agent, and participants were told the shared data would be published online. However, it is still not clear how this translates to realistic usage scenarios. Users may decide to share harmless data to gain money, even knowing that data will be published. This does not necessarily mean that they would share data in a realistic scenario with multiple issues under negotiation and more obscure rewards. The situation that is of more interest in the IoV, is what happens when users *have* to share *sensitive* data to obtain a particular service they want or need. This constitutes a significant challenge for the design, validation, and deployment of incentive mechanisms in the context of personal information negotiation. Current research cannot provide a robust answer today and has to be extended significantly to do so.

F. Multi-party Privacy

Due to the involvement of various parties, resolving multi-party privacy conflicts is challenging. Furthermore, the potential for multi-party privacy conflicts may instil doubt in the IoV and its services, and could render the IoV to be perceived as untrustworthy. The IoV could benefit from current research in social networks focusing on detecting and resolving privacy conflicts, when users have conflicting privacy preferences on a co-owned data item. Research in social media, which introduces the capability for users to compromise is listed in Table VIII. In more detail, in [112] users bid to decide who will determines the sharing decision for the item. However, as [113] note, users may have difficulty in understanding mechanism and in specifying appropriate bid values, plus bidding for each co-owned item can be cumbersome.

TABLE VIII
AN OVERVIEW OF MULTI-PRIVACY METHODS IN SOCIAL NETWORKS. NOTE THAT ALL APPLY IN NEGOTIATING THE SHARING DECISION FOR THE CO-OWNED DATA ITEM IN QUESTION.

Paper	Method
[112]	Auction to determine who makes the information-sharing decisions
[114]	Majority voting mechanism for conflict resolution
[115]	Veto voting mechanism for conflict resolution
[116]	Uploader decides the voting mechanism for conflict resolution
[117]	Automatic inference of the resolution method
[118]	Game theoretic method incorporating social pressure
[119]	Game theoretic method incorporating reciprocity

Further work is involved with voting mechanisms, where users vote for sharing the item or not. These votes are aggregated to reach an outcome with a majority mechanism in [114] and a veto voting mechanism in [115]. Various voting mechanisms are combined in [116] and the uploader decides which mechanism will be used, but this assumes that the uploader anticipates the consequences of sharing, and that there is no malicious intent [113]. In [117], the model chooses automatically among different negotiation methods taking into account the preferences of users, the sensitivity of the content, and the relationships among the audience for the content. Research has also considered the strategic interaction among participants in conflicts. However, [113] note that, although these approaches assume rationality, rationality is not necessarily observed in users' *actual* behaviour. Some approaches allow for social pressure [118] or reciprocity [119], but there are more social factors in multiparty privacy conflicts such as reputation, trust, and accountability [113].

However, it is important to note that multi-party privacy in the IoV is conceptually different from multi-party privacy in the social media. In social media, a conflict can occur due to data sharing among users, which includes data on other users. In comparison to this, we provided a more loose definition for multi-party privacy conflicts in the IoV in Section III-A. This is because the systematic collection of involuntary information in the IoV along with the IoV's large scale pose a significant risk also to the privacy of non users (e.g. see parking space identification in Section IV-C and on-demand video feeds in Section IV-H). It is thus very likely that users and non users will be largely unaware of multi-party privacy conflicts in the IoV, thereby only a small amount of conflicts will be able to be negotiated let alone resolved. This makes designing solutions resolve multi-party privacy conflicts very challenging in the IoV, and calls for comprehensive research. Furthermore, it stresses the necessity for privacy-by-design solutions which could enhance confidence in the IoV in the first place.

VI. Conclusions

Privacy in the Internet of Vehicles is an under-researched topic when it comes to end-user services such as parking space identification, platooning and intelligent intersections. At the same time, proposed services (discussed in Section IV) require multiple types of private data. To determine research gaps and classify issues, this paper has documented services in the IoV according to the types of information that is collected.

A thorough review of services reveals that sharing personal information can help, but may not be crucial for improving certain IoV services. For example, in Section IV-D it was discussed that it is possible to obtain very good estimates of traffic conditions by utilising anonymous data from a limited number of drivers. For other services, personal information does help but the incentives for end-users to provide this information are not always explained adequately. For instance, Section IV-G discussed that intelligent intersections may not necessarily be beneficial, especially in environments that include mixed vehicle types. At the same time, it will be difficult and obtrusive for drivers to manage privacy and to make informed decisions on sharing information. It is also an issue that—aside from compromising functionality—improving the privacy of services may also impact trust among service users.

Further research directions have been identified in Section V. Specifically, open research problems are: privacy-by-

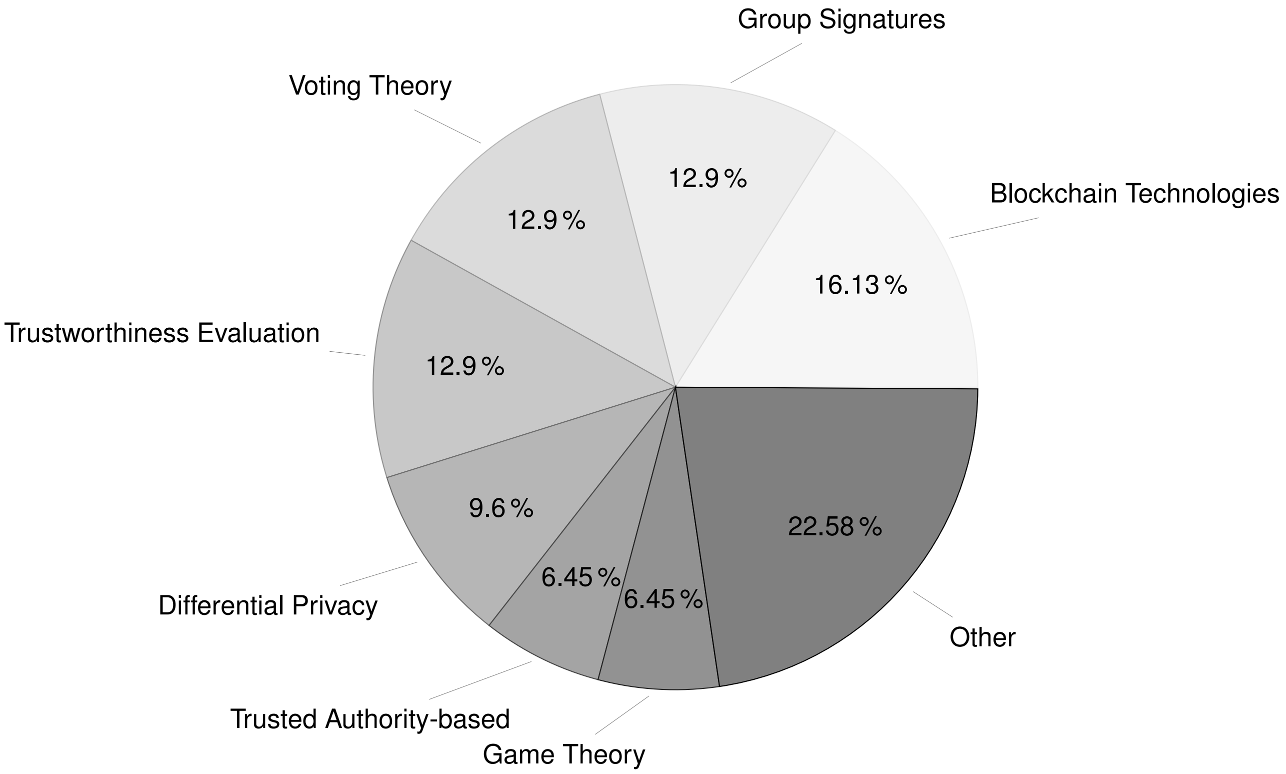

Fig. 1. Among the 31 papers that can help address privacy and trust issues in the IoV (in Tables VI-VIII), a large portion has to do with Blockchain technologies, Group Signatures, Voting Theory, Node Trustworthiness Evaluation, and Differential Privacy. Some of these further utilise Game Theory and Trust Authority-based service provision. With 'Other' we denote those approaches which are highly context specific or few in literature; that is work that utilises Privacy Labels, Virtual Trip Lines, Digital Forensics, Auctions, and Private Information Retreival.

design standardisation, establishing trust, incentives to provide information, measuring privacy and service quality trade off, consent negotiation and resolving multi-party privacy conflicts. This work has presented several approaches that can be used toward improving privacy and trust in the IoV, and a summary of the methods found is given in Figure 1. We especially believe that addressing multi-party privacy is highly significant. That is because it can affect both users of the IoV and non-users, making it difficult to track and address privacy conflicts, and easy to exploit information.

To conclude, dismissing privacy issues can lead to severe adverse effects due to the vast exchange of personal information in the IoV, as well as the large number of participants. It can result in the IoV being perceived as a monitoring system or as an intrusive technology. To alleviate such concerns and minimise opportunities for information exploitation in the IoV, it is crucial that academia, the industry, and policy makers make significant collaborative efforts to address the privacy issues and challenges this work has discussed.

References

[1] L. Campanile, M. Iacono, F. Marulli, and M. Mastroianni, "Privacy Regulations Challenges on Data-centric and IoT Systems: A Case Study for Smart Vehicles," in *Proc. 5th International Conference on Internet of Things (IoTBDS 2020)*, 2020.

[2] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Internet of Vehicles: An Introduction," *Int. J. Adv. Res. Comp. Sci. Software Eng.*, vol. 8, no. 1, p. 11, 2018.

[3] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.

[4] M. Gerla, E. K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum on Internet of Things, (WF-IoT '14)*, Seoul, South Korea, 2014.

[5] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of Internet of Vehicles," *China Commun.*, vol. 11, no. 10, pp. 1–15, 2014.

[6] W. Sun, "Internet of Vehicles," *Advances in Media Technology*, vol. 5, no. 2, pp. 47–52, Jan. 2013.

[7] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, "Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1314–1345, 2019.

[8] m. c. schraefel, R. Gomer, A. T. Alan, G. E. H., and M. Carsten, "The Internet of Things: Interaction Challenges to Meaningful Consent at Scale," *ACM Interactions*, vol. XXIV, no. 6, pp. 26–33, 2017.

[9] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, Mar. 2013.

[10] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, and Y. Xiong, "Security and Privacy in the Internet of Vehicles," in *Proc. International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI '15)*, Beijing, China, 2015.

[11] V. Tiwari and B. K. Chaurasia, "Security issues in fog computing using vehicular cloud," in *Proc. International Conference on Information, Communication, Instrumentation and Control (ICICIC, '17)*, Indore, India, Aug. 2017.

[12] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[13] Committee on Digital Economy Policy, OECD. (2014) Summary of the OECD Privacy Expert Roundtable. Accessed: Sep. 04, 2020. [Online]. Available:

https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en

[14] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for Vehicular Ad Hoc Networks," *Veh. Commun.*, vol. 1, no. 1, pp. 33–52, 2014.

[15] L. Silva, N. Magaia, B. Sousa, A. Kobusińska, A. Casimiro, C. X. Mavromoustakis, G. Mastorakis, and V. H. C. de Albuquerque, "Computing Paradigms in Emerging Vehicular Environments: A Review," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 3, pp. 491–511, 2021.

[16] I. Bhardawaj and S. Khara, "Research trends in Architecture, Security, Services and Applications of Internet of Vehicles (IOV)," in *Proc. International Conference on Computing, Power and Communication Technologies (GUCON 2018)*, Greater Noida, India, 2018, pp. 91–95.

[17] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Future Gener. Comput. Syst.*, vol. 88, pp. 16–27, 2018.

[18] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[19] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. T. Lin, and X. Liu, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[20] E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs," *Int. J. Distrib. Sens. N.*, vol. 12, no. 9, 2016.

[21] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social Internet of Vehicles: Architecture and enabling technologies," *Comput. Electr. Eng.*, vol. 69, pp. 68–84, 2018.

[22] L. Maglaras, A. Al-Bayatti, Y. He, I. Wagner, and H. Janicke, "Social Internet of Vehicles for Smart Cities," *J. Sens. Actuator Netw.*, vol. 5, no. 1, p. 3, 2016.

[23] K. M. Alam, M. Saini, and A. El Saddik, "Workload model based dynamic adaptation of social internet of vehicles," *Sensors*, vol. 15, no. 9, pp. 23 262–23 285, 2015.

[24] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, "Cognitive Internet of Vehicles," *Comput. Commun.*, vol. 120, pp. 58–70, 2018.

[25] K. I. Moharm, E. F. Zidane, M. M. El-Mahdy, and S. El-Tantawy, "Big Data in ITS: Concept, Case Studies, Opportunities, and Challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 8, pp. 3189–3194, Aug. 2019.

[26] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, 2012.

[27] Z. Li, Y. Chen, D. Liu, and X. Li, "Performance Analysis for an Enhanced Architecture of IoV Via Content-Centric Networking," *EURASIP J. Wirel. Comm.*, vol. 124, 2017.

[28] M. Nitti, L. Atzori, and I. P. Cvijikj, "Friendship selection in the social internet of things: Challenges and possible strategies," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 240–247, 2015.

[29] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[30] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, "A Cooperative Quality-Aware Service Access System for Social Internet of Vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2506–2517, 2018.

[31] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions," *IEEE Access*, vol. 7, pp. 79 694–79 713, 2019.

[32] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1654–1667, 2020.

[33] M. Barati, O. Rana, I. Petri, and G. Theodorakopoulos, "GDPR Compliance Verification in Internet of Things," *IEEE Access*, vol. 8, pp. 119 697–119 709, 2020.

[34] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, "A survey on security and privacy issues in IoV," *Int. J. Electr. Comput. Eng*, vol. 10, no. 5, pp. 5409–5419, 2020.

[35] X. Jia, L. Xing, J. Gao, and H. Wu, "A survey of location privacy preservation in social internet of vehicles," *IEEE Access*, vol. 8, pp. 201 966–201 984, 2020.

[36] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2018.

[37] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[38] G. G. Fuster, *The emergence of personal data protection as a fundamental right of the EU.* Springer Science & Business, 2014, vol. 16.

[39] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV)," in *Proc. IEEE International Congress on Internet of Things (ICIOT 2017)*, Honolulu, HI, USA, 2017, pp. 25–32.

[40] T. Zhang, H. Antunes, and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, 2014.

[41] W. Ben Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, "Fast and Secure Multihop Broadcast Solutions for Intervehicular Communication," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 433–450, 2014.

[42] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *Proc. 2010 IEEE Symposium on Security and Privacy (S&P 2010)*, 2010, pp. 447–462.

[43] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," *IACR Cryptology*, vol. 2010, p. 332, 2010.

[44] W. Ben Jaballah, M. Conti, M. Mosbah, and C. Palazzi, "Impact of security threats in vehicular alert messaging systems," in *Proc. 2015 IEEE International Conference on Communication Workshop (ICCW 2015)*, 2015, pp. 2627–2632.

[45] Y. Ma, Z. Wang, H. Yang, and L. Yang, "Artificial intelligence applications in the development of autonomous vehicles: a survey," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 2, pp. 315–329, 2020.

[46] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the Ratee: A Trust Management System for Social Internet of Vehicles," *Wirel. Commun. Mob. Comput.*, vol. 2017, 2017.

[47] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger, and S. Steinhorst, "Towards a Blockchain-based Identity and Trust Management Framework for the IoV Ecosystem," in *Proc. Global Internet of Things Summit (GIoTS 2020)*, Dublin, Ireland, 2020, pp. 1–6.

[48] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 2, pp. 426–441, 2020.

[49] C. Stach and B. Mitschang, "Privacy Management for Mobile Platforms – A Review of Concepts and Approaches," in *Proc. IEEE International Conference on Mobile Data Management (MDM '13)*, Milan, Italy, Jun. 2013.

[50] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Secur. Priv.*, vol. 3, no. 1, pp. 26–33, 2005.

[51] W.-C. Chiu, P.-H. Hsieh, W.-L. Wu, and C.-L. Lin, "Helmet-Mounted Display System of Motorcyclist with Collision Detecting and Navigation," in *Proc. International Conference on Internet of Vehicles (IOV '17)*, S.-L. Peng, G.-L. Lee, R. Klette, and C.-H. Hsu, Eds. Kanazawa, Japan: Springer International Publishing, Nov. 2017.

[52] C. F. Yang, Y. H. Ju, C. Y. Hsieh, C. Y. Lin, M. H. Tsai, and H. L. Chang, "iParking – a real-time parking space monitoring and guiding system," *Veh. Commun.*, vol. 9, pp. 301–305, 2017.

[53] S. Mathur, T. Jin, N. Kasturirangan, J. Chandrasekaran, W. Xue, M. Gruteser, and W. Trappe, "ParkNet: Drive-by Sensing of Road-side Parking Statistics," in *Proc. International Conference on Mobile Systems, Applications, and Services (MobiSys '10)*, San Francisco, CA, USA, 2010.

[54] Y.-L. Hu, C.-Y. Wang, C.-K. Kao, S.-Y. Chang, D. S. L. Wei, Y. Huang, I.-Y. Chen, and S.-Y. Kuo, "Toward Fog-Based Event-Driven Services for Internet of {Vehicles}: Design and Evaluation," in *Proc. International Conference on Internet of Vehicles (IOV '17)*, S.-L. Peng, G.-L. Lee, R. Klette, and C.-H. Hsu, Eds. Kanazawa, Japan: Springer International Publishing, Nov. 2017.

[55] J. Wan, J. Liu, Z. Shao, A. V. Vasilakos, M. Imran, and K. Zhou, "Mobile crowd sensing for traffic prediction in internet of vehicles," *Sensors*, vol. 16, no. 1, p. 88, 2016.

[56] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: Rich Monitoring of Road and Traffic Conditions Using Mobile Smartphones," in *Proc. Conference on Embedded Network Sensor Systems (SenSys '08)*, Raleigh, NC, USA, 2008.

[57] W. Zong, Z. Liu, S. Yang, Q. Yuan, and F. Yang, "Multi-Task Oriented Participant Recruitment for Vehicular Crowdsensing," in *Proc. International Conference on Internet of Vehicles (IOV '17)*, S.-L. Peng, G.-L. Lee, R. Klette, and C.-H. Hsu, Eds., Kanazawa, Japan, Nov. 2017.

[58] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden, "CarTel: A Distributed Mobile Sensor Computing System," in *Proc. International Conference on Embedded Networked Sensor Systems (SenSys '06)*, Boulder, Colorado, USA, 2006.

[59] K. Ali, D. Al-Yaseen, A. Ejaz, T. Javed, and H. S. Hassanein, "CrowdITS: Crowdsourcing in intelligent transportation systems," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC '12)*, Shanghai, China, Apr. 2012.

[60] T. Lei, S. Wang, J. Li, and F. Yang, "A cooperative route choice approach via virtual vehicle in IoV," *Veh. Commun.*, vol. 9, pp. 281–287, 2017.

[61] M. M. de Weerdt, S. Stein, E. H. Gerding, V. Robu, and N. R. Jennings, "Intention-Aware Routing of Electric Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1472–1482, May 2016.

[62] P. Dutta, "Coordinating rendezvous points for inductive power transfer between electric vehicles to increase effective driving distance," in *Proc. International Conference on Connected Vehicles and Expo (ICCVE '13)*, Las Vegas, NV, USA, 2013.

[63] H. Wang, Z. Li, X. Zhu, and Z. Liu, "A Full Service Model for Vehicle Scheduling in One-Way Electric Vehicle Car-Sharing Systems," in *Proc. International Conference on Internet of Vehicles (IOV '15)*, C.-H. Hsu, F. Xia, X. Liu, and S. Wang, Eds., Chengdu, China, Dec. 2015.

[64] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "RoadSpeak: Enabling Voice Chat on Roadways using Vehicular Social Networks," in *Proc. Workshop on Social Network Systems (SocialNets '08)*, New York, NY, USA, 2008.

[65] W. Sha, D. Kwak, B. Nath, and L. Iftode, "Social vehicle navigation: Integrating Shared Driving Experience into Vehicle Navigation," in *Proc. Workshop on Mobile Computing Systems and Applications (HotMobile '13)*, New York, NY, USA, 2013.

[66] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, "Mobeyes: Smart mobs for urban monitoring with a vehicular sensor network," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 52–57, Oct. 2006.

[67] M. Chen, F. Li, J. Lei, Z. Zeng, Q. Han, and Q. Chen, "Driving fatigue detecting method based on temperature insensitive ECG parameters," in *Proc. International Conference on Internet of Vehicles (IOV '17)*, S.-L. Peng, G.-L. Lee, R. Klette, and C.-H. Hsu, Eds. Kanazawa, Japan: Springer International Publishing, Nov. 2017.

[68] F. Browand, J. McArthur, and C. Radovich, "Fuel Saving Achieved in the Field Test of Two Tandem Trucks," UC Berkeley, Partners for Advanced Transportation Technology, California, Tech. Rep. UCB-ITS-PRR-2004-20, 2004.

[69] C. Bergenhem, Q. Huang, A. Benminoun, and T. Robinson, "Challenges of platooning on public motorways," in *Proc. World Congress on Intelligent Transport Systems*, Busan , South Korea, 2010.

[70] J. Kjellberg, "Implementing control algorithms for platooning based on V2V communication," Ph.D. dissertation, KTH Royal Institute of Technology, Stockholm, Sweden, 2011.

[71] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa, "Overview of platooning systems," in *Proc. World Congress on Intelligent Transpor Systems*, Vienna, Austria, Oct. 2012.

[72] S. Tsugawa, "Results and issues of an automated truck platoon within the energy ITS project," in *Proc. IEEE Intelligent Vehicles Symposium*, Dearborn, MI, USA, Jun. 2014, pp. 642–647.

[73] K. Dresner and P. Stone, "A Multiagent Approach to Autonomous Intersection Management," *J. Artif. Intell. Res.*, vol. 31, pp. 591–656, 2008.

[74] H. Kowshik, D. Caveney, and P. R. Kumar, "Provable Systemwide Safety in Intelligent Intersections," *IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 804–818, Mar. 2011.

[75] J. Lee and B. Park, "Development and Evaluation of a Cooperative Vehicle Intersection Control Algorithm Under the Connected Vehicles Environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 81–90, Mar. 2012.

[76] J. Wu, A. Abbas-Turki, and A. El Moudni, "Cooperative driving: An ant colony system for autonomous intersection management," *Appl. Intell.*, vol. 37, no. 2, pp. 207–222, Sep. 2012.

[77] D. Carlino, S. D. Boyles, and P. Stone, "Auction-based autonomous intersection management," in *Proc. IEEE Conference on Intelligent Transportation Systems (ITSC '13)*, The Hague, Netherlands, Oct. 2013.

[78] K. Kim and P. R. Kumar, "An MPC-Based Approach to Provable System-Wide Safety and Liveness of Autonomous Ground Traffic," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3341–3356, Dec. 2014.

[79] Q. Lu and K. Kyoung-Dae, "Intelligent Intersection Management of Autonomous Traffic Using Discrete-Time Occupancies Trajectory," *J. Traffic. Logist. Eng.*, vol. 4, no. 1, pp. 1–6, Jun. 2016.

[80] J. Cheng, W. Wu, J. Cao, and K. Li, "Fuzzy Group-Based Intersection Control via Vehicular Networks for Smart Transportations," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 751–758, Apr. 2017.

[81] B. Zheng, C. Lin, H. Liang, S. Shiraishi, W. Li, and Q. Zhu, "Delay-Aware Design, Analysis and Verification of Intelligent Intersection Management," in *Proc. IEEE International Conference on Smart Computing (SMARTCOMP '17)*, Hong Kong, China, May 2017.

[82] O. Barzilai, N. Voloch, A. Hasgall, O. L. Steiner, and N. Ahituv, "Traffic Control in a Smart Intersection by an Algorithm with Social Priorities," *Contemp. Eng. Sci.*, vol. 11, no. 31, pp. 1499–1511, 2018.

[83] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual Trip Lines for Distributed Privacy-preserving Traffic Monitoring," in *Proc. International Conference on Mobile Systems, Applications, and Services (MobiSys '08)*, Breckenridge, CO, USA, 2008.

[84] J. C. Herrera, D. B. Work, R. Herring, X. J. Ban, Q. Jacobson, and A. M. Bayen, "Evaluation of traffic data obtained via GPS-enabled mobile phones: The Mobile Century field experiment," *Transport. Res. C-Emer.*, vol. 18, no. 4, pp. 568–583, Aug. 2010.

[85] Z. Sun and X. J. Ban, "Vehicle trajectory reconstruction for signalized intersections using mobile traffic sensors," *Transport. Res. C-Emer.*, vol. 36, pp. 268–283, Nov. 2013.

[86] N. Marković, P. Sekuła, Z. V. Laan, G. Andrienko, and N. Andrienko, "Applications of Trajectory Data From the Perspective of a Road Transportation Agency: Literature Review and Maryland Case Study," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1858–1869, May 2019.

[87] S. Tsugawa, "An Overview on an Automated Truck Platoon within the Energy ITS Project," *IFAC Proc. Vol.*, vol. 46, no. 21, pp. 41–46, Jan. 2013.

[88] J. B. Michael, D. N. Godbole, J. Lygeros, and R. Sengupta, "Capacity Analysis of Traffic Flow Over a Single-Lane Automated Highway System," *J. Intell. Transport. S.*, vol. 4, no. 1-2, pp. 49–80, Jan. 1998.

[89] S. Kumar, L. Shi, N. Ahmed, S. Gil, D. Katabi, and D. Rus, "CarSpeak: A Content-centric Network for Autonomous Driving," in *Proc. Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM '12)*, Helsinki, Finland, 2012.

[90] J. Wang, H. Liu, H. Bao, B. Bennett, and C. Flores-Montoya, "Target Localization and Navigation with Directed Radio Sensing in Wireless Sensor Networks," in *Proc. International Conference on Internet of Vehicles (IOV '15)*, C.-H. Hsu, F. Xia, X. Liu, and S. Wang, Eds., Chengdu, China, Dec. 2015, pp. 101–113.

[91] L. Chen and C. Englund, "Cooperative Intersection Management: A Survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 2, pp. 570–586, 2016.

[92] Q. Li, F. Qiao, X. Wang, and L. Yu, "Drivers' smart advisory system improves driving performance at STOP sign intersections," *J. Traffic Transp. Eng.*, vol. 4, no. 3, pp. 262–271, Jun. 2017.

[93] UK Autodrive and Cambridge University. (2017) Study on user acceptance of driverless cars. Accessed: Sep. 04, 2020. [Online]. Available: http://www.ukautodrive.com/survey-finds-uk-public-still-open-minded-about-self-driving-vehicles

[94] Deloitte Global Automotive. (2020) Exploring Consumer Trends on the Future of Automotive Retail. Accessed: Sep. 04, 2020. [Online]. Available: https://www2.deloitte.com/us/en/pages/manufacturing/articles/automotive-trends-millennials-consumer-study.html

[95] G. Sikander and S. Anwar, "Driver Fatigue Detection Systems: A Review," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 6, pp. 2339–2352, Jun. 2019.

[96] Z. Tan, C. Wang, C. Yan, M. Zhou, and C. Jiang, "Protecting Privacy of Location-Based Services in Road Networks," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–14, 2020.

[97] J. M. Abowd, "How Will Statistical Agencies Operate When All Data Are Private," *J. Priv. Confidentiality*, vol. 7, no. 3, May 2017.

[98] A. Wood, M. Altman, A. Bembenek, M. Bun, M. Gaboardi, J. Honaker, K. Nissim, D. R. O'Brien, T. Steinke, and S. Vadhan, "Differential Privacy: A Primer for a Non-Technical Audience," *Vanderbilt J. Entertain. Technol. Law*, vol. 21, pp. 209–276, 2018.

[99] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating Noise to Sensitivity in Private Data Analysis," in *Proc. Theory of Cryptography Conference (TCC '06)*, New York, NY, USA, Mar. 2006.

[100] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme," in *Proc. Advances in Cryptology (CRYPTO 2000)*, 2000, pp. 255–270.

[101] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang, "Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions," in *Proc. Advances in Cryptology (ASIACRYPT 2016)*, 2016, pp. 373–403.

[102] R. Xe, C. He, C. Xu, and C. Gao, "Lattice-based Dynamic Group Signature for Anonymous Authentication in IoT," *Ann. Telecommun.*, vol. 74, pp. 531–542, 2019.

[103] K. Gu, W. Zhang, S.-J. Lim, P. K. Sharma, Z. Al-Makhadmeh, and A. Tolba, "Reusable Mesh Signature Scheme for Protecting Identity Privacy of IoT Devices," *Sensors*, vol. 20, no. 3:758, 2020.

[104] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Commun. Surveys Tus.*, vol. 22, no. 2, pp. 1191–1221, 2020.

[105] P. Zhang and M. Zhou, "Security and Trust in Blockchains: Architecture, Key Technologies, and Open Issues," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 3, pp. 790–801, 2020.

[106] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5g-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7940–7954, 2020.

[107] W. Yong-hao, "A Trust Management Model for Internet of Vehicles," in *Proc. 4th International Conference on Cryptography, Security and Privacy (ICCSP 2020)*, 2020, pp. 136–140.

[108] T. Baarslag, A. T. Alan, R. Gomer, M. Alam, C. Perera, E. H. Gerding, and m. schraefel, "An Automated Negotiation Agent for Permission Management," in *Proc. International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '17)*, S&#227;o Paulo, Brazil, 2017.

[109] T. Baarslag, M. Kaisers, E. H. Gerding, C. M. Jonker, and J. Gratch, "Computers That Negotiate on Our Behalf: Major Challenges for Self-sufficient, Self-directed, and Interdependent Negotiating Agents," in *Proc. International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '17)*, S&#227;o Paulo, Brazil, 2017.

[110] W. C. Li, M. Nirei, and K. Yamana, *Value of data: there's no such thing as a free lunch in the digital economy*. RIETI, 2019.

[111] G. Malgieri and B. Custers, "Pricing privacy–the right to know the value of your personal data," *Computer Law & Security Review*, vol. 34, no. 2, pp. 289–303, 2018.

[112] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective Privacy Management in Social Networks," in *Proc. International Conference on World Wide Web (WWW '09)*, Madrid, Spain, 2009.

[113] J. M. Such and N. Criado, "Multiparty Privacy in Social Media," *Commun. ACM*, vol. 61, no. 8, pp. 74–81, Aug. 2018.

[114] B. Carminati and E. Ferrari, "Collaborative access control in on-line social networks," in *Proc. International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom '11)*, Orlando, USA, Oct. 2011.

[115] K. Thomas, C. Grier, and D. M. Nicol, "unFriendly: Multi-party Privacy Risks in Social Networks," in *Proc. International Symposium on Privacy Enhancing Technologies (PETS '10)*, M. J. Atallah and N. J. Hopper, Eds., Berlin, Germany, Jul. 2010.

[116] H. Hu, G. Ahn, and J. Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 7, pp. 1614–1627, Jul. 2013.

[117] J. M. Such and N. Criado, "Resolving Multi-Party Privacy Conflicts in Social Media," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 7, pp. 1851–1863, Jul. 2016.

[118] S. Rajtmajer, A. Squicciarini, J. M. Such, J. Semonsen, and A. Belmonte, "An Ultimatum Game Model for the Evolution of Privacy in Jointly Managed Content," in *Proc. International Conference on Decision and Game Theory for Security (GameSec '17)*, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds., Vienna, Austria, Oct. 2017.

[119] D. Kekülluöglu, N. Kökciyan, and P. Yolum, "Strategies for Privacy Negotiation in Online Social Networks," in *Proc. International Workshop on AI for Privacy and Security (PrAISe '16)*. The Hague, Netherlands: ACM, Aug. 2016.

Efstathios Zavvos received his PhD in Computer Science from the University of Southampton in 2019. He has studied several Artificial Intelligence areas including Machine Learning, Intelligent Agents, Game Theory, Genetic Algorithms and Expert Systems. He is currently the Head of Artificial Intelligence at VLTN BV. His recent research interests include charging station investor competition, the Internet of Vehicles and connected vehicles, digital twins, and logistics planning and optimisation.

Enrico H. Gerding is an Associate Professor in the Agents, Interaction and Complexity research group in the Department of Electronics and Computer Science at the University of Southampton. He has been an academic at Southampton since 2007. He received his PhD from the Dutch National Centre of Mathematics and Computer Science in 2004 on the topic of automated negotiation. He has over 100 peer-reviewed publications in top conferences, journals and books in the area of artificial intelligence, specifically autonomous agents and multi-agent systems.

Vahid Yazdanpanah is a postdoctoral Research Fellow in the Agents, Interaction and Complexity research group in the Department of Electronics and Computer Science at the University of Southampton. He received his PhD from the University of Twente on the application of multiagent techniques for implementing industrial collaborations. His general research focus is on intelligent agent technologies, decision support concepts, and formal methods for multiagent systems. In particular, he is interested in modelling the behaviour of multiagent systems, logical frameworks to represent and reason about decision processes, and sociotechnical aspects of responsibility reasoning in multiagent settings.

Carsten Maple is a Professor of cyber systems engineering with the Warwick Manufacturing Group, The University of Warwick, where he is also the Director of research in cyber security. He has an international research reputation having published over 200 peer-reviewed papers. His research, widely reported through the media, has attracted millions of pounds in funding. He is currently a Principal Investigator (PI) with the EPSRC/GCHQ Academic Centre of Excellence in Cyber Security, a Local PI of the U.K. Research Hub for Cyber Security of the Internet of Things, PETRAS, and FAIRSPACE, and the U.K. Research Hub for Future AI and Robotics in Space, and a Co-Investigator of the CARMA project, all funded by EPSRC. His research interests include authentication, privacy, the value of information, and cyber-physical systems. He is a fellow of the Alan Turing Institute.

Sebastian Stein is an Associate Professor within the Agents, Interaction and Complexity research group, which is part of Electronics and Computer Science at the University of Southampton. He completed his PhD in Multiagent Systems at Southampton in 2008 and he is a Turing AI Fellow. Sebastian's research focuses on techniques from mechanism design, incentive engineering, and sequential decision making, and their application for solving real-life problems in smart mobility, smart energy, crowdsourcing, and cloud computing.

m.c. schraefel is a Professor of Computer Science and Human Performance, Fellow of the British Computer Society, and Research Chair for the Royal Academy of Engineering. Her research focuses on the design information systems to support the brain-body connection for quality of life, including fitness to learn, play and perform, and to understand through these paths how to enhance innovation, creativity and discovery. She also directs the WellthLab, whose vision is to help make normal better for all. The lab's mission is to develop the science, engineering, and design of human-centred, human-systems interaction, from individual to infrastructure, that empowers people to explore, define, build, and own their own healthful cultures.