

Privacy Protection of Automated and Self-Driving Vehicles

Frank Kargl^{*1}, Ioannis Krontiris^{*2}, Jason Millar^{*3},
André Weimerskirch^{*4}, and Kevin Gomez^{†5}

1 Universität Ulm, DE. frank.kargl@uni-ulm.de

2 Huawei Technologies – München, DE. ioannis.krontiris@huawei.com

3 University of Ottawa, CA. jmillar@uottawa.ca

4 Lear Corporation, US. aweimerskirch@lear.com

5 TH Ingolstadt, DE. Kevin.Gomez@carissma.eu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 23242 “Privacy Protection of Automated and Self-Driving Vehicles”. While privacy for connected vehicles has been considered for many years, automated and autonomous vehicles (AV) technology is still in its infancy and the privacy and data protection aspects for AVs are not well addressed. Their capabilities pose new challenges to privacy protection, given the large sensor arrays that collect data in public spaces and the integration of AI technology.

During the seminar, several keynote presentations highlighted the research challenges from different perspectives, i.e. legal, ethical, and technological. It was also discussed extensively why vehicles need to make dynamic assessments of trust as an enabling factor for the secure communication and data sharing with other vehicles, but without increasing any privacy risks.

Then, the main objective of the seminar was to produce a research road-map to address the major road-blockers in making progress on the way to deployment of privacy protection in automated and autonomous vehicles. First, the group identified six common scenarios of Cooperative, Connected and Automated Mobility (CCAM) during development and product life-cycle, and analyzed the privacy implications for each scenario. Second, it formulated the need to have a methodology to determine the cost-benefit trade-offs between privacy and other criteria like financial, usability, or safety. Third, it identified existing tools, frameworks, and PETs, and potential modifications that are needed to support the automotive industry and automotive scenarios. Finally, the group explored the interplay between privacy and trust, by elaborating on different trust properties based on performance, on ethical aspects, and on user acceptance.

Seminar June 11–16, 2023 – <https://www.dagstuhl.de/23242>

2012 ACM Subject Classification Security and privacy → Human and societal aspects of security and privacy; Security and privacy → Privacy protections; Security and privacy → Privacy-preserving protocols

Keywords and phrases Automotive Security and Privacy, Privacy and Data Protection, Cooperative Connected and Automated Mobility

Digital Object Identifier 10.4230/DagRep.13.6.22

* Editor / Organizer

† Editorial Assistant / Collector



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 4.0 International license

Privacy Protection of Automated and Self-Driving Vehicles, *Dagstuhl Reports*, Vol. 13, Issue 6, pp. 22–54
Editors: Frank Kargl, Ioannis Krontiris, Jason Millar, André Weimerskirch, and Kevin Gomez



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Frank Kargl (Universität Ulm – Ulm, DE)

Ioannis Krontiris (Huawei Technologies – München, DE)

Jason Millar (University of Ottawa, CA)

André Weimerskirch (Lear Corporation – Ann Arbor, US)

License © Creative Commons BY 4.0 International license

© Frank Kargl, Ioannis Krontiris, Jason Millar and André Weimerskirch

Cooperative, connected and automated mobility (CCAM) has the potential to drastically reduce accidents, travel time, and the environmental impact of road travel. To achieve these goals, automated vehicles (AV) will require a range of sensors and communication devices that receive and read extensive data from the vehicle's environment, as well as machine learning algorithms that process this data. This immediately raises the concern of privacy for AVs. A first Dagstuhl Seminar was held virtually January 23–28, 2022 [1], and identified four main challenges: (1) How to encourage stakeholders to follow proper ethics and responsible behaviour, (2) how regulation needs to evolve for CCAM systems, (3) the commercial limitations to develop and implement proper privacy protection, and (4) availability of privacy-enhancing technologies for CCAM systems. The Dagstuhl Seminar at hand was then held in person June 11–16, 2023, with the goal to approach those main challenges.

This seminar was organized in a number of expert presentations, and then the group split into four working groups. The expert presentations covered many relevant aspects around regulation and governance, cloud-based support infrastructure, and technology. The four working groups roughly map to the main challenges:

1. **Scenarios, Risks, Impacts, and Collected Data in CCAM:** This group identified six common CCAM scenarios during development and product life-cycle, and analyzed the privacy implications for each scenario. Some of these scenarios are unique to CCAM privacy and set it apart from other areas. The results can now be used as foundation for further general in-depth privacy research.
2. **Privacy Tensions for Connected Automated Vehicles:** It is believed that privacy comes at a cost, whether it is a financial cost, reduced usability, or reduced safety. It is essential to understand how to find the acceptable trade-off between privacy and the considered criteria. However, today we have no proper methodology in place to determine proper trade-off points, and therefore this group worked on developing such a methodology. Additionally, this group will identify the technology readiness level of privacy enhancing technologies (PET) to support the trade-off points. The working group plans to describe details in an upcoming scientific publication.
3. **Automotive Privacy Engineering:** Privacy engineering provides the underlying tools, frameworks, and technologies to develop privacy protecting CCAM. This working group focused on identifying existing tools, frameworks, and PETs that could support our use-case, potential modifications that are needed to support CCAM, and gaps. The group emphasized the need to match the privacy engineering to users' privacy and usability expectations. The group identified and discussed six questions that addressed the major aspects, and derived various action items for the automotive privacy research community.
4. **Interplay between Privacy and Trust:** One of the most important milestones in order to achieve the shared vision on the deployment of Cooperative Intelligent Transport Systems (C-ITS) towards cooperative, connected and automated mobility (CCAM), is to allow

participating entities to assess dynamically the trustworthiness of the shared information, in order to be able to rely on it and coordinate their actions [2]. In addressing this complex issue, it's paramount to strike a balance between enhancing trust and ensuring the privacy and security of users' personal information and data. The group explored the interplay between privacy and trust, by elaborating on different trust properties based on performance, on ethical aspects, and on user acceptance.

We conclude that more solution-oriented research and development is required to establish privacy modeling tools and privacy engineering specifically for CCAM, and we hope that the results and papers coming from this seminar will support the journey to privacy protecting CCAM. Shortly after the seminar, the Mozilla Foundation's Privacy Not Included [3, 4] reviewed 25 major car brands for consumer privacy and gave all of them failing marks for consumer privacy, and we hope that this seminar's solutions also improve the privacy of next generation passenger vehicles.

References

- 1 Frank Kargl, Ioannis Krontiris, Nataša Trkulja, André Weimerskirch, and Ian Williams, Privacy Protection of Automated and Self-Driving Vehicles (Dagstuhl Seminar 22042), Dagstuhl Reports, Vol. 12, Issue 1, pp. 83–100, <https://doi.org/10.4230/DagRep.12.1.83>.
- 2 EU Project “CONNECT: Continuous and Efficient Cooperative Trust Management for Resilient CCAM”, [ONLINE] <https://horizon-connect.eu/>
- 3 Mozilla Foundation, “Privacy Nightmare on Wheels”: Every Car Brand Reviewed By Mozilla – Including Ford, Volkswagen and Toyota – Flunks Privacy Test, [ONLINE] <https://foundation.mozilla.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/>
- 4 Mozilla Foundation, Privacy Not Included, [ONLINE] <https://foundation.mozilla.org/en/privacynotincluded/categories/cars/>

2 Table of Contents

Executive Summary

Frank Kargl, Ioannis Krontiris, Jason Millar and André Weimerskirch 23

Overview of Talks

Exploring the Costs of AVs and Privacy

Adam Henschke 26

A Quick Intro to AD Regulations

Ben Brecht 26

The Automotive Industry under Worldwide Data Protection Regulations:

A Technical Perspective

Alaa Al-Momani 27

Demystifying the Tension between Trust and Privacy in CCAM

Thanassis Giannetsos 28

Privacy Challenges in Vehicle Security Operation Centers – From a CCAM perspective

Kevin Gomez 28

PQC Impacts on V2X

Takahito Yoshizawa and Brigitte Lonc 29

Technology, Data, and Enforcement in Service to Autonomy and Community

Bryant Walker Smith 30

Working Groups

Working Group on Scenarios, Risks, Impacts, and Collected Data in CCAM

Kevin Gomez, Adam Henschke, Bryant Walker, Brigitte Lonc, Ben Brecht, Stefan Gehrler, Christos Papadopoulos 32

Working Group on Privacy Tensions for Connected Automated Vehicles

Jonathan Petit, Jason Millar, Sarah Thorton, Michael Buchholz, Zoltan Mann . . . 40

Automotive Privacy Engineering

Ala'a Al-Momani, David Balenson, Christoph Bösch, Kyusuk Han, Mario Hoffmann, Sebastian Pape, Nataša Trkulja, Takahito Yoshizawa 41

Interplay between Privacy and Trust


Thanassis Giannetsos, Frank Kargl, Ioannis Krontiris, Francesca Bassi, Anje Gering 49

Participants 54

3 Overview of Talks

3.1 Exploring the Costs of AVs and Privacy


Adam Henschke (University of Twente, NL)

License  Creative Commons BY 4.0 International license
© Adam Henschke

I introduced a range of ethical issues about AVs (autonomous vehicles) and privacy that arise in relation to insurance. Tesla vehicles in some US states now offer a “safety score” which impacts their Tesla provided insurance. This seems good as it incentivises safer driving and reduced insurance premiums. However, there are problems like phantom braking, in which false information (AV braking when it does not need to) has an effect of unfairly raising driver’s insurance premiums. This application highlights that AVs present a unique set of privacy risks and challenges. For instance, there are economic incentives to collect behavioural data on drivers. Second, this approach to individualising/personalising insurance costs runs the risk of “responsibilisation”, in which individuals are held responsible for systemic issues, like poorly maintained road: An individual’s safety score may drop if they drive on poorly maintained roads, even if they are not the cause of those poorly maintained roads and can do nothing individually to repair them. By looking at safety scores and insurance, we have a useful way to think about a wide range of privacy issues when considering AVs.

3.2 A Quick Intro to AD Regulations

Ben Brecht (Berlin, DE)

License  Creative Commons BY 4.0 International license
© Ben Brecht

With the adoption of (EU) 2022/1426 [1] and (EU) 2022/2236 [2] as an amendment to the EU Whole Vehicle Type Approval Framework, type approval of an SAE Level 3 or 4 autonomous vehicle is possible for the first time in Europe. Type Approval is not sufficient to operate an autonomous vehicle in Europe. This requires an adapted national framework, as the EU has no legislative competence for the registration of vehicles and thus for the approval of an operating area. In Germany, this has been achieved through adjustments to the Road Traffic Act (StVG)[3], the Compulsory Insurance Act, the Vehicle Registration Ordinance (FZV)[4] and the creation of the Autonomous Vehicles Approval and Operation Ordinance (AFGBV)[5]. Specifically, the AFGBV contains the rules for the operating area permit, which is a mandatory requirement for road registration of L3/L4 vehicles after the revision of the FZV. For the permission to transport passengers, a concession according to the Passenger Transport Act (PBefG)[6] is additionally required.

All these regulations impose requirements on the generation, storage, processing or sharing of data (e.g. with authorities). A deeper look at the requirements from (EU) 2022/1426 with extensions of the list of data to be stored in the Event Data Recorder according to Article 6 of Regulation (EU) 2019/2144[7] reveals a rather traditional approach, which ignores data from cameras, lidars and radars. These data are also not taken into account in the requirements for reporting to authorities, although they are indispensable for the analysis of safety-relevant incidents. Only in the requirements for a safety management system (SMS), there is a very broad scope for the storage and processing of data, but – after a first rough technical analysis – it seems restrictions on purpose or use of such data might be missing.

References

- 1 Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles. *Official Journal, L 221, 26.8.2022, p. 1–64.*
- 2 Commission Delegated Regulation (EU) 2022/2236 of 20 June 2022 amending Annexes I, II, IV and V to Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the technical requirements for vehicles produced in unlimited series, vehicles produced in small series, fully automated vehicles produced in small series and special purpose vehicles, and as regards software update. *Official Journal, L 296, 16.11.2022, p. 1–176.*
- 3 Road Traffic Act (Straßenverkehrsgesetz) [ONLINE] <https://www.gesetze-im-internet.de/stvg/BJNR004370909.html>
- 4 Verordnung über die Zulassung von Fahrzeugen zum Straßenverkehr (Fahrzeug-Zulassungsverordnung – FZV) [ONLINE] https://www.gesetze-im-internet.de/fzv_2023/BJNR0C70B0023.html
- 5 Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung – AFGBV) [ONLINE] <https://www.gesetze-im-internet.de/afgbv/BJNR098610022.html>
- 6 Personenbeförderungsgesetz (PBefG) [ONLINE] <https://www.gesetze-im-internet.de/pbefg/BJNR002410961.html>
- 7 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users [ONLINE] <https://eur-lex.europa.eu/eli/reg/2019/2144/oj>

3.3 The Automotive Industry under Worldwide Data Protection Regulations: A Technical Perspective

Alaa Al-Momani (Ulm University, DE)


License © Creative Commons BY 4.0 International license
© Alaa Al-Momani

The recent adoption of data protection regulations is necessary to regulate how and for what purpose consumers' data is collected, processed, and shared. Generally, organisations that collect, process, or share personal information of data subjects are required to comply with one (or more) data protection regulations. In the case of the automotive industry and its various services, collecting as well as processing and sharing (sensitive) personal information is highly likely, including identifiers and geolocation of end-users. In this talk, we compare the data protection regulations in major automotive industry markets around the world, ie, the European Union (EU), the United States of America (US), and Japan. In particular, we look at the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Japanese Act on the Protection of Personal Information (APPI), respectively, and discuss the impact of these regulations on automotive services. We consider an autonomous taxicab service as an example of an automotive service and investigate how

such a service can be designed in compliance with the previous regulations. We further highlight the challenge that a worldwide service provider faces when complying with all of the previous regulations at once as they may substantially differ in some aspects. Furthermore, we take a look at the road ahead and highlight the challenges when it comes to integrating machine learning models and artificial intelligence within automotive services.

3.4 Demystifying the Tension between Trust and Privacy in CCAM

Thanassis Giannetsos (UBITECH Ltd. – Athens, GR)

License  Creative Commons BY 4.0 International license
© Thanassis Giannetsos


Modern vehicles are no longer mere mechanical devices; they comprise dozens of digital computing platforms coordinated by an in-vehicle network, and have the potential to significantly enhance the digital life of individuals on the road. While this transformation has driven major advancements in road safety and transportation efficiency, significant work remains to be done to capture the strict security, privacy, and trust requirements of all involved stakeholders.

For instance, driving on the road requires trust in others and the environment, but in reality, we never completely trust – not us, not other drivers or what is ahead of us. Therefore, how can we be sure about the data integrity and level of trust in connected cars that cooperatively need to execute a safety-critical function? At the same time, the integration of such integrity and assurance controls might impede with the privacy profile of the vehicles which, in turn, might affect the level of user acceptance of such systems – user perceived trust is greatly affected by the system’s capability to preserve the privacy of the driver.

In this presentation, we had a deeper look into the details of trust management vs. privacy and why vehicles need to make dynamic assessments of trust as an enabling factor for the secure communication and data sharing with other CCAM entities, but without increasing any privacy risks. EU Project CONNECT has shown a complete framework how this is technically possible. At the end we achieve the end-goal of combing a vehicle’s systems with information available externally (from multiple sources), in a way that expand the knowledge on the environment that is required for decision-making, in a trustworthy but also privacy-friendly way. This increases the safety of the overall CCAM ecosystem and unlocks future applications.

3.5 Privacy Challenges in Vehicle Security Operation Centers – From a CCAM perspective

Kevin Gomez (Technical University Ingolstadt, DE)

License  Creative Commons BY 4.0 International license
© Kevin Gomez

The SELFY project develops a toolbox for the CCAM environment. We (THI) develop a Vehicle Security Operation Center (VSOC) for the SELFY toolbox and CCAM environments. The SELFY VSOC can be considered a meta VSOC that collects data from various endpoints within the vehicle ecosystem and provides services to the ecosystem and vehicle manufacturers. Those services include the detection of anomalies, distribution of information (e.g., security scenarios and MITRE ATT&CK matrix), updates, and trust scores.

One of the main challenges within the VSOC is the trustworthiness of OEMs. Why should an OEM trust the SELFY VSOC? What is the benefit of sharing information with the SELFY VSOC? And how can we, as the SELFY VSOC, trust data from the endpoints and OEMs?

One solution to tackle the challenge could be differential privacy. Here, data can be shared while individuals without identifying the OEM as a participant in the dataset. This characteristic would address challenges by OEMs with external systems such as the SELFY VSOC. An OEM could share data with the SELFY VSOC without being identified as a participant and potentially leaking information on their security scenarios, vulnerabilities, and used technologies. However, privacy does not come without additional costs. In differential privacy, the degree of privacy depends on a factor, usually referred to as epsilon. “How much data does one need for effective different privacy in a VSOC?”, “Is the distrust from OEMs solved by differential privacy?” and “What epsilon should be chosen for which data types?”.

3.6 PQC Impacts on V2X

Takahito Yoshizawa (KU Leuven, BE) and Brigitte Lonc (IRT SystemX, FR)

License © Creative Commons BY 4.0 International license
© Takahito Yoshizawa and Brigitte Lonc

Vehicular communication, or Vehicle-to-Everything (V2X) communication uses digital signature called Elliptic Curve Digital Signature Algorithm (ECDSA) to verify the message’s integrity and sending vehicle’s authenticity. Its signature and public key lengths are 64 and 32 bytes, respectively. At the same time, Due to the evolving capabilities of Quantum Computers (QC), public-key cryptography (e.g. RSA, ECC) are expected to be broken when the QC of sufficient computing power become available. According to several articles, QCs as large as 100,000 qubits may become available by 2030 [1, 2]. If this becomes a reality, some of the expressed concerns may become an imminent issue [3, 4].

To address this issue, US National Institute of Standards and Technology (NIST) started standardizing work of Post-Quantum Cryptography (PQC) in 2016. As of today, 3 PQC signature algorithms are standardized [5]. However, all of them have large signature and/or public key size which saturates the V2X message size [6, 7]. In light of this situation, NIST invited call for proposal (CFP) for additional PQC signature algorithm that has characteristics of short signature and fast verification [8]. According to their current schedule, we may have viable solution(s) identified in early 2025, which may be suitable for real-time systems such as V2X communication.

References

- 1 Wikipedia.org, “Timeline of quantum computing and communication”, [ONLINE] https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication.
- 2 MIT Technology Review, “IBM wants to build a 100,000-qubit quantum computer”, [ONLINE] <https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/>
- 3 J. Proos, C. Zalka, “Shor’s discrete logarithm quantum algorithm for elliptic curves,” *Quant. Inf. Comput.*, vol. 3, no. 4, pp. 317–344, Jul. 2003.
- 4 NIST IR 8105, “Report on Post-Quantum Cryptography”, Apr. 2016

- 5 NIST, IR8413 “Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process”, <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf>.
- 6 B. Lonc, X. Aubry, H. Bakhti, M. Christofi, H.A. Mehrez, “Feasibility and Benchmarking of Post-Quantum Cryptography in the Cooperative ITS Ecosystem”, IEEE Vehicular Networking Conference (VNC 2023), April. 2023.
- 7 T. Yoshizawa, B. Preneel, “Post-Quantum Impacts on V2X Certificates – Already at The End of The Road”, IEEE Vehicular Technology Conference (VTC 2023), June 2023.
- 8 NIST, “Post-Quantum Cryptography: Digital Signature Schemes”, [ONLINE] <https://csrc.nist.gov/projects/pqc-dig-sig>

3.7 Technology, Data, and Enforcement in Service to Autonomy and Community

Bryant Walker Smith (University of South Carolina – Columbia, US)

License  Creative Commons BY 4.0 International license
© Bryant Walker Smith

Privacy is about power and, as a means rather than an end, should be discussed in relation to the twin societal goals of human autonomy and community.

As an initial matter: While the state of automated driving has for years been overhyped, currently it is underappreciated. Today there is much reason for technical optimism, even as economic success is challenging. But technical or even economic success is not the same as social or policy success. For example, automated driving could become widespread even if it is not privacy-protecting – an outcome which may or may not be socially desirable.

These policy discussions are happening now. For example, dozens of countries in the UN’s Global Forum for Road Traffic Safety are currently exploring a new international instrument on automated driving. Privacy has been a flash point in this effort and its predicates. Some of the especially interesting issues arise from cross-border dynamics of the vehicle or its automated driving system, relevant data, and notions of “control.” I describe some of these specific scenarios.

To my thesis: Privacy is an incomplete frame. Some people prioritize acceptance, belonging, validation, or legacy over privacy. There are also tradeoffs within as well as with privacy: The victim of a drunk driver has a privacy interest in not being hit, stripped naked and touched for emergency surgery, and dependent on assistance for the remainder of their life. More fundamentally, privacy is a negative right based on antagonistic relationships: “The right to be left alone.” It is defensive rather than optimistic.

The twin goals of human autonomy and community are more inclusive and inspiring than privacy alone. Autonomy is the freedom to discover oneself, be true to oneself, and live one’s own life; it requires some, but not complete, privacy. Community is connection with others, which often depends on “frictions” in life, such as interacting with strangers. While autonomy and community are in some tension, they are both part of happiness in the sense of leading a good life (eudaimonia). And so it may be more helpful to ask what promotes these goals, which might require data protection or data sharing. This is often a question of power, and in general power and privacy should be inversely related: The more powerful a person or a company is, the fewer privacy protections they should enjoy in law.

Several additional points from my talk last year can ground our discussions. First, focus these discussions by considering what is and is not unique about automated driving, what distinctions with respect to data collection and use might be helpful, and the various actors

against whom one might assert a privacy interest. Second, safety offers a useful analogy for privacy, especially because a key question for both is whether the company behind a given technology is trustworthy (rather than whether the technology itself is trusted). Third, one of the key policy choices is who or what will be empowered: individuals, governments, companies, or other collectives – that is, communities. Artificial intelligence has a role here, especially in connecting and magnifying those with common interests. These points are further explained in last year’s abstract.

A key example of these power dynamics is law enforcement. Far too many people die and are injured on our roads. This has led to a “safe systems approach” to traffic safety. Enforcement of traffic laws is also highly flawed, including in ways that demand a “safe and just approach” to this enforcement. Automated enforcement is part of this approach. It also raises a key question: Is there a difference between ideal enforcement and perfect (that is, complete) enforcement? I discuss case studies including graduated licensing, intoxication detection, and automated enforcement.

Private enforcement in combination with automation is especially striking. Imagine an automated driving company that punishes a wayward pedestrian by restricting that person’s access to the company’s automated driving services or even its other services. More generally, companies with evidence of a legal violation will choose how to interact with law enforcement – by sharing such data with police or the public at large without prompting, by demanding some private or public process for release of these data, or by seeking to make such release impossible. They may also be skeptical or deferential in their posture toward legal processes to order such release. A particular concern of power is when governments and companies “team up” with each other against individuals on matters of privacy. Some antagonism between these potentially powerful actors is helpful!

The safe systems approach can inspire and inform a “grand unified theory of enforcement.” It involves thinking systematically and strategically, enforcing upstream, cultivating norms, and designing for feedback. I discuss each of these principles at length.

4 Working Groups

4.1 Working Group on Scenarios, Risks, Impacts, and Collected Data in CCAM

Kevin Gomez (Technische Hochschule Ingolstadt, DE)

Adam Henschke (University of Twente, NL)

Bryant Walker Smith (University of South Carolina – Columbia, US)

Brigitte Lonc (IRT SystemX, FR)

Ben Brecht (Berlin, DE)

Stefan Gehrler (Robert Bosch LLC, Pittsburgh, US)

Christos Papadopoulos (University of Memphis, US)

License © Creative Commons BY 4.0 International license

© Kevin Gomez, Adam Henschke, Bryant Walker, Brigitte Lonc, Ben Brecht, Stefan Gehrler, Christos Papadopoulos

Our working group was interested in exploring the following set of issues related to Continuous Connected Automated Mobility/Autonomous Vehicles (CCAM/AVs)¹: presenting scenarios to recognize and express the risks and potential impacts of collected data, examining whether there are unique features of *automotive privacy* that set it apart from other areas where information technologies may impact privacy, and discuss how law enforcement and international geopolitical issues distinguish CCAM/AVs from traditional discussions on legacy automotive vehicles and systems. The group's primary focus was on identifying scenarios, risks, impacts, and collected data in CCAM/AVs, which will serve as a foundation for further in-depth research to better understand the relationship between privacy and CCAM, considering the highlighted characteristics.

4.1.1 Discussed Problems

Our aim was to engage in a series of structured discussions that would facilitate the development of scenarios to identify and explain privacy issues in the context of CCAM/AV. We followed the following method: Each participant presented a set of questions to structure the subsequent analysis. We then presented various cases or issues that highlighted privacy-relevant concerns. In this process, we identified key stakeholders who might be vulnerable to privacy issues, whose activities could impact privacy, or who would be responsible for responding to such issues. Subsequently, we created a generalized scenario that outlined the key steps in CCAM/AV development and public release, allowing us to provide specific detailed examples relevant to privacy concerns. These examples were then organized into thematic clusters, as presented in Table 1. Building on this, we offer suggestions on how this analysis and thematic clustering can aid in identifying and communicating privacy issues in CCAM/AVs.

¹ A note on nomenclature: We use here the terms CCAM/AVs to capture issues in both connected automated driving and autonomous vehicles. While these terms may refer to different sets of technologies, they are also sometimes used interchangeably. Given that they are used differently and can refer to different sets of technologies whilst also referring to overlapping technologies, we consider that CCAM/AVs is a valuable way of encompassing the broader sets of discussions in which both CCAM and AVs present challenges for privacy. Note, however, that in connected versus autonomous driving, a lot of CCAM infrastructure might gather data that is independent of/orthogonal to AVs, i.e. CCTV, licence matching, intersection management, etc.

Following, we identified various structuring questions:

- Should there be any surveillance tools built into CCAM/AVs that actively help law enforcement?
- Should there be any restrictions on what LEOs (Law Enforcement Officers/Organisations) can access from CCAM/AVs?
- Who/what groups own vehicles and/or data?
- What sort of data is being discussed? Such as
 - Data in vehicle
 - Data outside the vehicle
 - Publicly collected data
- How to recognize and understand new sorts of data that can be gathered in CCAM/AVs, specifically medical/health data?
- What are the cybersecurity issues presented by CCAM/AVs? Such as
 - Misbehaviour detection
 - OEM outsourced services and cloud services
 - OEMs doing cloud services,
- What are the impacts on informed consent/privacy/confidentiality etc?
- Are CCAM/AVs considered critical infrastructure?
 - Noting that: If CCAM/AVs are designated as critical infrastructure, there may then be a need to share information with relevant national security institutions and LEOs, including the sharing of data in industrial control systems
- How to balance between the needs of LEO and the needs of customers or individuals?
- What role should an OEM play in this?
- (Why) is automotive privacy special from traditional driving with legacy vehicles and/or distinct from other information-gathering devices like smartphones?

Before delving into scenarios, risks, impacts, and collected data, the working group meticulously identified stakeholders in CCAM. We initiated the list with stakeholders for automotive digital forensics, as defined by Gomez Buquerin and Hof [1], considering that CCAM provides a relevant environment for such practices. However, we recognized that additional stakeholders were pertinent to this context beyond those identified by Gomez Buquerin and Hof. Thus, the final list of stakeholders is provided below: [list of stakeholders].

- Insurer (e.g., DEKRA, Allianz)
- Approval authority (e.g., UNECE approval entity)
- Business car owner (e.g., Telecom, Qualcomm)
- Criminal (e.g., cybercriminal, state-sponsored attacker group)
- OEM (e.g., Volkswagen, Toyota, General Motors)
- Legal institution (e.g., police)
- Researchers (e.g., research institutes, universities)
- Supplier (e.g., Bosch, Continental)
- Tuner (e.g., MTM, Brabus)
- Private car owner
- Mobility provider (e.g., Uber, Lyft), including renters/fleet managers
- Road infrastructure
- Government:
 - Bureaucratic
 - Regulatory
 - Investigative

- Third parties:
 - Pedestrians
 - Passengers
 - Emergency responders
 - Road construction
 - Any individuals/groups that provide remote assistance/remotely facilitate (automated) driving,
 - End-of-life issues (particularly concerning remnant data),
 - Lawyers
 - Cyber-security actors
 - People borrowing a car
 - Leased car (owned by the bank)

The government as a stakeholder sparked discussions within the working group. Since the government acts on behalf of the population (in democratic countries), they should not have their own stake in privacy aspects of CCAM. However, the working group decided to add the government as a stakeholder due to its involvement in bureaucratic, regulatory, and investigative aspects.

Based on the stakeholders, we defined various scenarios where privacy is impacted or at risk in CCAM. Those are:

- In Germany, BMW as a police entity, change the vehicles for a police car. New vehicles are now not being rebuilt; how can ex-police vehicles safely delete information when selling after service?
- Capacity to use data in the wheel sensor TPMS IDs global IDs from the sensor in the tire.
- Privacy for autonomous vehicles is unique because of the scale of data – time, amount, and range of data (more potent than NEST), and the computing resources have significant storage, communication, and analytic power.
- Ownership of vehicles/data derived from it. Issue of fleets/transportation as a service.
- Are CCAM/AVs to be understood as a product or a service?
- Insurance – Are you insuring the driver or the system? Insurance companies push for the owner of data as being the owner of the data so that they can get ownership over that information.

4.1.2 Possible Approaches

Consider now a case of a safety incident involving a test vehicle on a public street. As part of the forensic investigation, the data gathered by the test vehicle may be requested to identify the factors around the safety incident and perhaps to identify individuals or groups who may be held culpable or deserving of some redress. A range of potential stakeholders would be affected by/involved in the privacy analysis. They would include:

- OEM/Research team; those gathering data, those storing the data and/or those with access to the data
- Government; investigators such as local police
- Third parties; Pedestrians, Emergency responders, other road users, lawyers,

The information being accessed would include the following:

- Visual data
- (Raw) sensor data
- Internal bus data
- Personally identifiable information (PII)

Consider now a case of a cybersecurity incident in which PII gathered as part of testing and evaluation was at risk of either being exfiltrated or altered. Misbehavior detection tools have identified that a database of test data had been the target of the attack, and now it must be established if this cyberattack was successful and if there are any privacy implications arising from it. A range of potential stakeholders would be affected by/involved in the cybersecurity investigation and any subsequent privacy concerns. They would include:

- OEM/Research team; those gathering data, those storing the data and/or those with access to the data
- Government; investigators such as cybersecurity forensic investigators/CERTs etc.
- Third parties; drivers involved in the vehicle testing, pedestrians, other road users, lawyers

Consider now a case where a CCAM/AVs service provider unintentionally identifies criminal behaviour in a fleet car/shared car. As part of this service, in-vehicle cameras and microphones monitor abnormal behaviour and will record events inside the vehicle to either recognize health events (such as a heart attack) or serious safety risks (violent activity between passengers). In this case, two vehicle occupants pretend to wrestle, activating the in-vehicle surveillance. Once activated, the occupants are recorded consuming controlled substances and discussing where they got them. It turns out that the substances were legal in one state, but now the vehicle has crossed state lines, and the substances are now illegal. The in-vehicle surveillance and recording would affect a range of potential stakeholders here. They would include:

- Third parties; vehicle passengers, lawyers
- Government; investigators including LEOs
- OEM; does the OEM that is monitoring non-private vehicles have a responsibility to report this illegal activity? Are they permitted to volunteer this information? What level of privacy should occupants in “non-private but not public spaces reasonably expect?
- What, if any role, does the passage from one jurisdiction to another play in the expectations of the passengers, the responsibility of the investigators, and the permissions of the OEM?

4.1.3 Conclusions

We identified various privacy implications on the different phases of the development and product life-cycle of modern vehicles, their functions, and services. The following tables (Table 1, Table 2, Table 3, Table 4, Table 5, Table 6) summarizes those.

References

- 1 Kevin Gomez Buquerin; Hans-Joachim Hof, *Identification of automotive digital forensics stakeholders*, SECURWARE 2021, The Fifteenth International Conference on Emerging Security Information, Systems and Technologies, p. 8-13 , 2021.

■ **Table 1** Identified privacy issues in test fleet data collection.

Test fleet data collection	Is it in public or not?
	Chilling effects/experimentation
	Informality/rush to market/security as a later/afterthought
	Foreign data leakage/national security
	Where is the data stored/location/entity
	Should we collect everything – gauge engineering inclination to collect all
	UN regulation 155, must follow more than security best practice
	Need safety compliance to meet standing orders of NHTSA, including reporting on prototypes, safety incidents
	Risks of shared/open data sets
	Public's first impressions/foundational artefact

■ **Table 2** Identified privacy issues in in-car data collection and back-end communication.

In-car data collection and back-end communication	Where is the data stored and how safe is it?
	Unauthorized access (entities, individuals etc.)
	Authorized access (entities, individuals etc.)
	Data retention policy including storage period
	Choices about what to track during processing
	Retention of raw data versus retention of processed data
	Potential for anonymization (when, where, and whether)
	Issues in security of communication of information/transfer/data accessibility means and methods
	Integrity of data set: Use and manipulation of data/data integrity/chain of custody/documentation
	Explainability/transparency/trust

■ **Table 3** Identified privacy issues in training and testing algorithms.

Training and testing algorithms	Pitfalls in machine learning, things like bias (sampling, parameters, inappropriate baseline)
	Inappropriate assumptions (i.e. threat model)
	Data insecurity: Find out what data was used to train the ML, black box or white box, you can then use that to infer the training data, model inversion from data leaking, remnant personally identifiable information, membership
	Deanonimisation
	Use of synthetic versus real data (privacy versus safety/accuracy)
	Imperfect approaches to anonymization
	Third party partners, especially labelling/post-processing
	Limitations of anonymization
	Digital twinning
	Lack of understanding of privacy implications of privacy (i.e. gait/walk might be privacy revealing)
	Overuse of data (might as well use, might need to use given algorithm, design pathways)
	Metadata

■ **Table 4** Identified privacy issues in making and producing products or services.

Making and producing products or services	Meeting/not meeting privacy requirements (e.g., GDPR), cybersecurity requirements etc., noting that they are different by jurisdiction
	Products of services that are incidental to AD (i.e., health monitoring)
	Product or services that necessarily involve PII (i.e., health monitoring)
	Pressures inherent in low profit margins
	Seeing/setting privacy as a goal or as a constraint, new limitations or design criteria, trade-offs between different components (given need to save money/cents per unit)
	Conflicts/trade-offs between marketers, managers, and engineers, i.e. over-promising (WRT privacy, promising services that are/potentially in conflict with privacy)
	Privacy requirements (i.e. GDPR) that may be different given different jurisdiction
	Need to have inactivated privacy features (anticipated for a particular jurisdiction)
	Supply chain complexities and data disputes (e.g. android auto)
	Over the air updates/right to repair introducing/perpetuating vulnerabilities, hardware dependencies
	Open versus closed systems
	“Software defined cars”: subscription features/subscription model of service provision, in vehicle marketing
	Legacy systems – both privacy and cybersecurity vulnerabilities
	Factory/location of production locations, i.e. issues of supply chain integrity
	Simplicity versus complexity – is the solution to security/privacy to create really complicated systems or really simple systems

■ **Table 5** Identified privacy issues in after market operations.

After market operations	Data leftovers – shared car/leased car (i.e. police example) arising from multiple users
	Oversharing by parents/friends/relatives etc.,
	Road user privacy and
	Changing/disrupted concepts of privacy
	Inside vehicle (driver/owner, passengers), other road users in vehicles, other road users not in vehicles, PII from other vehicles
	No more service – who is responsible for ongoing privacy after OEM responsibility ends
	Buying privacy/monetizing privacy (inequities/fairness)
	Non vehicle privacy invasive infrastructure (i.e. intersection management, verification of ongoing operational safety), V2V, V2X communications etc.
	Used vehicles changing jurisdictions – vehicles systems designed for the privacy demands of one country moving to another country
	Updates
	General operations
	Re-purposing data, look for additional models/sources, desperation to monetize, corporate end of life
	Metadata and data creep
	Reporting and investigations of safety incidents
	Change of ownership
	Particular (public spaces and semi-public transport)
	Outsourcing the monitoring
	Companies cooping privacy i.e. good faith arguments of privacy are exploited, to resist the sharing of information, bad faith, NY goes to Uber wants to understand where people are travelling through the day, but Uber says no because they want to sell it, but use privacy as the excuse not to sell it
	Who owns the data
	Geopolitics – i.e., gathering national security significant surveillance data, economic competitions
	New privacy regulations that come up that need to be fulfilled/met
	Ongoing responsibility for OEMs, is the driver/owner responsible to update or not?
	Complex supply chains and streams of commerce
	Privacy related incidents and who is responsible? OEM, supplier, individual
	Mandatory reporting for cybersecurity events
	Cross border travel/enforcement
	Cyber-security incidents
	Cyber-security versus privacy trade-offs
	Vehicles as attractive targets, fleets at scale

■ **Table 6** Identified privacy issues in selling and releasing products or services.

Selling and releasing products or services	Over promising and hyping
	Pressures to take product to market, we can fix it later (issues more for engineers for early release)
	Downstream confusion (dealers etc.), Upselling of privacy risking components/- salesperson incentives
	Challenges for customer – mass and length of privacy policies
	Informed consent and ongoing responsibilities
	Legalistic notion of informed consent shifting responsibility to customer
	One off consent model versus dynamic and ongoing consent models, ongoing notion of consent
	Adam's conspiracy theories/trust issues
	Point of sale – When a vehicle is being constantly updated, when is the point of sale? (Software defined vehicles)
	Who is the customer/customers?
	Issues around fleet models – who is the customer/who is setting the privacy expectations (user, employer, business etc.)
	Disruption in the responsibilities of the salesperson – can a salesperson/should a sales person have to assess the competence of a customer's capacity to give informed consent – medical bioethics model
	Risk of information overload and decisions/consent fatigue
	Marketing pressures and the desire/incentive to say that everything is fine – competitive pressures on marketers
	Broad notion of supply chain integrity
	Tricky to sell privacy (because it is risk based rather than reward based)

4.2 Working Group on Privacy Tensions for Connected Automated Vehicles


Jonathan Petit (Qualcomm, USA)

Jason Millar (University of Ottawa, CA)

Sarah Thorton (NURO, USA)

Michael Buchholz (Ulm University, DE)

Zoltan Mann (University of Amsterdam, NL)

License  Creative Commons BY 4.0 International license

© Jonathan Petit, Jason Millar, Sarah Thorton, Michael Buchholz, Zoltan Mann

4.2.1 Context and Objective

A common belief is that privacy comes at a cost, and hence, a tension exists between achieving full privacy and full “performance”. This tension can be seen as finding the acceptable trade-off between privacy and the considered value/criteria. Let us consider the case of an automated vehicle driving in a city. To ensure road safety, an automated vehicle needs to detect pedestrians with high accuracy. Moreover, for accurate prediction and planning, the vehicle should be able to differentiate between different types of pedestrian, e.g., children, adult, impaired users. Indeed, depending on the user type, the motion model used by the behaviour prediction algorithm is adjusted. However, a privacy goal is to minimize those attributes. Therefore, a privacy-enhancing technology could only allow to output the coarse object “pedestrian”, thus conflicting with the “required” granularity.

In order to comprehensively discuss the privacy tensions, the working group identified the lack of a common methodology. The objective of the group was then to propose a methodology.

4.2.2 Methodology

The objective of the methodology is twofold. First, to capture and rate the privacy tensions (positive or negative). Second, because identifying the privacy tensions is an iterative process, it is useful to understand the current coverage of the analysis. So the methodology should also output a coverage/completion value.

The proposed methodology follows an 5-steps approach. Note that this is a work-in-progress and will be refined in a future publication.

1. Specify use case: describe the scenario, its objective(s).
2. Identify stakeholders: list direct and indirect user/actors.
3. For each stakeholder, list respective assets, privacy needs and performance objectives.
4. Rate impact of dimension on privacy.
5. Assess current coverage/completion of the analysis for each dimension.

4.2.3 Conclusion

Creating a methodology to analyze privacy tensions (or synergies) is paramount to capture each dimensions (e.g., security, ethics, efficiency) and identify the technology readiness level of appropriate PETs. In a forthcoming publication, we will refine the methodology and validate it by applying it to case studies such as automated delivery service.

4.3 Automotive Privacy Engineering

Ala'a Al-Momani (Ulm University, DE)

David Balenson (USC Information Sciences Institute, US)

Christoph Bösch (Robert Bosch GmbH, DE)

Kyusuk Han (Technology Innovation Institute, Abu Dhabi, AE)

Mario Hoffmann (ARRK Engineering GmbH, DE)

Sebastian Pape (Continental Automotive Technologies, DE)

Nataša Trkulja (Ulm University, DE)

Takahito Yoshizawa (KU Leuven, BE)

License © Creative Commons BY 4.0 International license

© Ala'a Al-Momani, David Balenson, Christoph Bösch, Kyusuk Han, Mario Hoffmann, Sebastian Pape, Nataša Trkulja, Takahito Yoshizawa

Privacy engineering forms one of the core aspects to develop privacy-friendly products and services. Many components of privacy engineering and privacy-by-design have been introduced lately, yet their applicability to the automotive domain is still in its early stage. One example of privacy-by-design in vehicular communication is the 5GAA's whitepaper [1].

Our overarching goal in this working group is to identify existing or needed tools and frameworks to help commercial entities comply with regulations by embedding privacy into their products, and how the available tools can be adapted and tailored toward the automotive industry. A major part of this includes investigating how privacy engineering can be embedded in the software or product development life cycle. Furthermore, we aim to explore whether privacy strategies, as introduced by Hoepman [3] as well as privacy patterns [4] are applicable in the automotive industry and automotive scenarios in a straightforward manner, or whether certain modification is necessary to better suit special requirements in such scenarios. Moreover, we look into privacy enhancing technologies (PETs) and investigate whether these – once implemented – could achieve the system's functionality without introducing negative consequences due to specific automotive use cases, and at what cost PETs can be incorporated in a company's vision or implemented in its products.

To this end, it is of ultimate necessity to combine this technological and strategic privacy engineering effort with users' expectations and their behaviour when it comes to privacy protection.

This includes how a vehicle driver and passengers can be educated about vehicle data usage and, more importantly, its privacy implications, and how other road users and non-vehicle entity's privacy such as pedestrians' can be addressed. Intuitive design of user interfaces (UIs) needs to be used to ensure informed decisions about certain options for driver's or passengers' privacy. This may go beyond traditional consent forms that graphically appear on, e.g., webpages or mobile apps, to include other forms of human machine interaction (HMI) such as audio. The goal of such design should maximize transparency and avoid privacy dark patterns [5] in any UI design.

In the following, we discuss the questions addressed in this working group followed by our recommendations to enhance the applicability of privacy engineering in the automotive domain.

4.3.1 Discussion Questions

In this working group, we identify and discuss six questions that address some of the major aspects of privacy engineering in the automotive domain.

Q1. What tools and frameworks are there to help commercial entities comply with regulations and embed privacy?

Our goal here is to identify privacy tools that have already been applied to automotive, in addition to identifying and investigating the applicability of general privacy engineering tools to automotive.

We begin by pointing out that privacy in automotive is distinctive due to several factors such as the limited storage and processing power, specific protocols related to vehicle connectivity and communication (e.g., CAN bus), and the direct interaction with human safety among other trade-offs. In addition, automotive scenarios often rely on certain sensitive data and information such as location data and driving behaviour requiring privacy protection. We refer the reader to [2] for additional information about automotive data. A noteworthy point to consider here is that the entire automotive ecosystem is very complex. Modern architecture of automotive systems include vehicles, mobile devices, communications, and third-party connected services such as infotainment services. Furthermore, vehicles come with a complex supply chain consisting of multiple layers, for which privacy must be considered with different responsibility, accountability, and liability. To illustrate this, we consider an ASIL-like certification program made for privacy. It is yet unclear whether such a program would be available at different levels, OEM-level, Tier-1, Tier-2 (Privacy Certificate for suppliers) or it would be for OEMs only.

In the privacy engineering landscape, there exist various tools and frameworks that have the potential to be used in the automotive domain. Examples of such include LINDDUN [13] as a privacy threat modelling framework, privacy design strategies, privacy patterns [4], and various privacy-enhancing technologies. Conducting a threat assessment and risk assessment (TARA) in the automotive domain may require considering different scopes of OEMs and suppliers along with the need to have a hierarchical analysis with a privacy impact assessment (PIA) on vehicle level supported by PIAs on component levels. This could also lead to a split of responsibility and tasks. For example, on a vehicle-level there needs to be a data strategy while on a component-level the task is more focused on implementing a PET.

One source of inspiration for the automotive privacy engineering community to consider are adjacent domains such as IT, mobile systems, and e-health. Ideas may be inspired by investigating the privacy engineering challenges of those domains and investigate if the solutions addressed the challenges in those domains can be transferred.

In the next questions, we will dig deeper into certain tools and frameworks of privacy engineering and investigate how to adapt and tailor them towards the automotive industry.

Q2. How to tailor privacy patterns to automotive industry, including what privacy patterns are there for automotive and leveraging architecture patterns?

In this question, we want to particularly investigate whether current privacy strategies and privacy patterns [4] are directly applicable to the automotive domain.

In order to address this question thoroughly, we recommend the community to identify a set of automotive use cases and assess the applicability of existing patterns and define how to adapt such applicable patterns. We note that it may also be necessary to develop new patterns specific to vehicles, taking into account vehicle architectural patterns and the privacy challenges in future use cases, e.g., for automated driving and shared robo-taxis.

In this working group, we aim to provide an initial assessment of the applicability of patterns in the automotive domain. We randomly choose three privacy patterns from the pattern repository [4] and, on a high-level, investigate their applicability to certain automotive scenarios.

Awareness Feed This pattern states the importance of providing information to the end user concerning their privacy. However, in the automotive scenarios and particularly, the direct applicability of such a pattern in the vehicle to inform the user is challenging as this may divert the driver's attention and thus may lead to an unsafe situation in cases of not fully automated driving scenarios.

To this end, it is important to identify when it is a good time to show the drivers certain privacy information in a way that does not interrupt their attention on driving. This may include innovative and unorthodox methods of informing end users, such as vibrating the steering wheel, or usage of audio channels.

Applying this pattern is also challenging if we consider informing other users, such as passengers of a car/taxi/bus. How to ensure such users are aware, are able to give consent, or select certain privacy preferences remain unsolved. The topic is even more complex for other road users, which can be communicated with even harder.

Informed Secure Passwords This pattern requests to ensure end users select strong and long passwords with various characters for different services and applications. However, given that the UIs available in cars nowadays do not match those of mobile phones and keyboards, it is very challenging and critical to apply this pattern directly in the vehicle. It is generally hard to type passwords in current vehicle interfaces. This opens the door to different solutions to enter passwords in vehicles, or even to question the usability of passwords as authentication method in vehicles. The automotive privacy community needs to investigate other forms of authentication such as physical authentication tokens (e.g. Yubikeys), or bio-metric information, and assess whether these are better fit to the automotive use cases. Other challenges include identity management and having different profiles/roles for a certain identity, e.g., a business and a private profile.

Location Granularity This pattern deals with location data and states that precise locations should be used with less granularity, e.g., street, ZIP code or city name, if precise location is not needed. On a first glance, we foresee a direct applicability for automotive scenarios, but we point out that the applicability is context-dependent, i.e., what level of granularity is needed for the context and thereafter it needs to be set. One example is a difference in the granularity requirements for finding a nearby restaurant in comparison to ordering a taxi for pickup. In the first example, the rough area is sufficient to receive information from a service about restaurants. The latter requires a more specific rendezvous point to make sure passenger and taxi can meet.

Q3. How can privacy engineering be embedded into the product or software development life cycle (SDLC) including threat modelling and verification of implementation?

The privacy engineering process defined by Hoepman [11] should be applied and integrated into the SDLC. Furthermore, extended SDLC models for privacy such as the W-model [18] and the σ -model [19] should be applied. Such models extend classical SDLC used in automotive industry like the V-model to include privacy-by-design phases. Another more challenging problem is the integration of privacy-enhancing technologies into agile environments [20, 21], since PETs are hard to compose. There seems to be a lack of privacy methodologies in the right-hand side of the V-model, i.e., the testing phases. We note that formulating testing and evaluation is challenging for privacy aspects, but not only in the automotive domain. Often, there is no external data available at the time of testing a certain privacy objective, and this heavily depends on

the context and on the runtime environment [10].

Q4. Can PETs achieve system’s functionality without blocking a certain functionality and at what cost can PETs be implemented in a company or a product?

Different PETs have been proposed in the literature, to name a few:

Multi-Party Computation (MPC): Several parties in a system collaboratively compute an agreed upon function where respective inputs are secret.

(Fully) Homomorphic Encryption ((F)HE): FHE supports the computation on encrypted data without the need to decrypt it.

Differential Privacy (DP): By adding noise into the analysis output, it formalizes and measures how much privacy is brought relative to losing utility.

K-anonymity: Masking data such that every record is indistinguishable from $k - 1$ other records in a dataset.

Trusted Execution Environments (TEEs): Areas in processing units with secure interaction with the rest of the system where data is encrypted outside but decrypted inside this environment.

Attribute-Based Credentials (ABC): Credentials, based on attributes instead of identities, allowing anonymous credentials for role-based access control (RBAC) or attribute-based access control (ABAC). Selective disclosure of attributes forms a key to achieving anonymous authentication.

Zero-Knowledge Proofs (ZKPs): Proving whether a statement is correct or not without leaking more information.

We note that this is only a subset of PETs, further PETs that might be used in automotive scenarios are listed by Garrido *et al.* [7] [Tab. II, p. 3; Tab. III, p. 4]. Garrido *et al.* discuss PETs in automotive use cases and conclude that there is still the need for a deep understanding of the use cases and the proposed PETs. A noteworthy remark is that in some cases, more than one PET needs to be applied to achieve an overarching privacy goal.

It is ultimately necessary to investigate whether PETs can be used generally in automotive scenarios without reducing functionality. More particularly, without impacting trust, safety, and other distinctive aspects of the automotive domain.

Let’s consider another possible scenario: cooperative intersection management using mobile edge computers. In this scenario, the edge, ideally, needs to know who you are, where you want to go, and your current position. In this scenario, the vehicle’s position is needed but not a link to the driver’s identity. **HE** may be used to compute the positions and directions in an encrypted fashion, but as a time-critical application, this may greatly impact the flow of traffic and the safety of road users. Considering that multiple vehicles are present in the vicinity with a known function to calculate, **MPC** might be useful.

Another solution to this scenario could be based on **ABC**, or privacy-preserving signature schemes, while using the minimal set of data needed in cleartext, e.g., the current location, velocity, steering angles, vehicle size category (e.g., car, bus, or truck with trailer), and the desired direction at the intersection (i.e., left, straight, right, or u-turn). This data could be used anonymously, i.e., without the vehicle, driver, and passenger identities. It would only be required to verify that the data truly originates from a valid vehicle, e.g., through the use of attribute-based credentials, or privacy-preserving signature schemes. However, it is worth noting that repetitive usage of accurate vehicle’s data such as the

vehicle's exact dimensions and direction of movement over a long period of time may increase the possibility of re-identification of that vehicle and/or driver [8].

To sum up, it is challenging to determine whether PETs may or may not be directly applicable in automotive scenarios and which one to use [7, 9]. Applying a PET in an application or a scenario requires clearly defining functionality requirements, privacy requirements, threat models, the bigger context of the systems and protocols involved in automotive scenarios.

Q5. What are people's privacy behaviours and expectations: how can vehicle users be educated about vehicle data usage and its implication? What about the privacy of extravehicular entities (pedestrians, etc.)?

In order to foster widespread adoption of privacy-friendly automotive features and scenarios, creating a demand from customers is crucial. This requires understanding the current people's perception of privacy when it comes to the automotive domain. Consequently, it is necessary to raise the awareness of privacy among customers to create the needed demand that will foster the deployment of privacy technologies into automotive scenarios.

The automotive privacy community needs to take into account the differences in people's perception of privacy that could stem from, e.g., cultural aspects based on regions or countries, which may impact how privacy options and controls can be designed and aligned with users' expectations. Therefore, we recommend conducting user studies on privacy expectations and actions specifically in the automotive space while taking into account cultural differences.

Additionally, we discussed the uniqueness of the automotive space over other domains such as mobile phones. This uniqueness may include further privacy-related factors such as driving behaviours and (in-cabin) cameras. Such additional factors would necessitate creating awareness of what data is collected, what PII is, and what seemingly is not PII, but can still be used to identify individuals or their driving patterns. The latter may be used to determine insurance rates or for re-identification of individuals using different vehicles in order to create and observe movement patterns. Thus, user awareness is essential in a transparent manner. When considering autonomous driving, different perceptions to the ones we discussed so far could be based on the level of autonomy. For example, at levels 4 and 5 there may not be any human driving pattern. However, privacy can be still an issue in new ways, such as user profiling in the car including, e.g., eye gazes, looking out the window, touching the steering wheel, etc.

Also, we need a comprehensive understanding of people's privacy perceptions under different use cases, that could be when users use their own car or using a shared car. The case of passengers' privacy needs also to be addressed adequately, that is, how passengers' privacy can be protected. To this end, this would require novel approaches of HMI considering the specific and uniqueness of the automotive domain. Enhancing customer awareness may take various forms and approaches. For example, the Vehicle Privacy Report website [12], provides privacy car facts for free by searching your VIN. It is necessary to study the best ways to increase user awareness and provide them with tools to learn about, understand, and adjust their privacy settings. One possibility is the "app" used for the scenario of shared car service. Another example that may be helpful to develop and use is the standardized privacy labels analogous to the energy-efficiency rating of consumer products, such as TV, fridge, etc. This links to the idea of a privacy score [15].

In fact, it is the tendency to collect data by default at any time when a new technology or service is deployed. Service providers will collect any and all data until they are told otherwise, for example, by regulators. On the other hand, regulating privacy can be very difficult. Even with privacy by default, providers will find a way around the regulation. Also, demands from the people themselves are needed to lead regulators to take action, bringing non-functional requirements like privacy as close to functional requirements and regulations.

We figure out the criteria for a user-friendly website, which includes “Easy to use”, “intuitive”, and “non-deception” (i.e., dark patterns [5, 6]). We need to tailor and apply such criteria to the automotive space, e.g. [14].

In summary, we consider that just relying on traditional privacy techniques may not be sufficient for automotive use cases. We encounter new challenges and need new creative ways for HMI, consent, informing, setting regulations, and preventing unwanted capture. Ultimately, we want people to drive knowing what’s allowed without being deceived or tricked. Privacy labels and scores might be helpful to consider in this case.

Q6. How can privacy controls (options) be designed in a way that maximizes transparency and avoids dark patterns in the UI?

Given the specifics in the automotive context we discussed previously, we understand that providing information with long text should be avoided, instead, informative videos could be used. We need to consider providing alternatives to match different users, as some people prefer text, while others may prefer pictures or videos.

Informing the user versus legally binding may be two different things. Does it need to be text to be legally binding? Should the legal agreement be done at the same time when the user is informed about data handling? As of today, it seems to be the practice that information and legally binding consent are handled together. Thus, these texts are often written by lawyers and are hard to understand for the users. If those two actions are split, who would write the “understandable” text or create the video? Still Lawyers? Or, the Marketing team or Independent parties? Eventually, this leads to lots of questions about this process.

It was also unclear when would be the best time to inform the users respectively get their consent. When the car is purchased? Every time the door is opened? When setting up the car and occasionally repeated as a reminder? When there are updates? In general, users get tired of seeing the same notices and warnings and eventually start to ignore them, as we are currently observing with the cookie banners on web pages. How would the passengers be informed or give their consent?

Clearly, we need an independent authority to define some kind of privacy metrics and scores. Ideally, manufacturers (and customers) should respond to these metrics and define their privacy controls accordingly.

Lengthy and detailed information may not be available at the moment the personal data is being used. Also, people may not understand how the data is being processed and what can be derived from it, even if detailed explanations are provided. (Will transparency still apply here?)

Which data is really needed for a service? Given the current usage of “Legitimate interest”, where service providers claim the need for all kinds of data for service improvement, marketing, and other analyses, it would be interesting to measure and identify the “bare minimum” of data needed: Given a certain scenario, based on the current state of the art what would be the minimum of data needed to provide a specific service?

4.3.2 Conclusion

Our working group sought to identify existing or needed tools and frameworks to help commercial entities comply with regulations by embedding privacy into their products, and how the available tools can be adapted and tailored toward the automotive industry. We explored six questions that address some of the major aspects of privacy engineering in the automotive domain, including identifying available tools and frameworks, tailoring privacy patterns, embedding privacy engineering in the SDLC, applying PETs to achieve needed functionality, learning about user privacy behaviour and expectation, and maximising transparency and avoiding dark patterns.

Throughout our discussion, we identified various action items that we believe are necessary to be addressed by the automotive privacy research and engineering community:

- a. There is a need to confirm, adapt, reject existing privacy strategies and patterns. (cf. Question 2) in terms of their applicability to the automotive domain.
 - i. It is necessary to identify appropriate privacy strategies (i.e., Minimize, Hide, Separate, Abstract, Inform, Control, Enforce, Demonstrate) and confirm that the existing eight strategies are appropriate and complete in the automotive space.
 - ii. Within this context, it is necessary to determine which existing privacy patterns are valid and usable in the automotive context, which ones have to be adapted, and which ones are missing and need to be added.
 - iii. Once the strategies and patterns are properly adapted to automotive context, then there is a need to map the privacy patterns to the steps of the development or product life cycle. (cf. Question 3)
- b. Identify a set of automotive scenarios, including connected cars and autonomous driving scenarios, and analyze which data is the *bare minimum* needed for the functionality of the service, including the use of PETs. Additionally, identify and derive upper and lower bounds where possible. (cf. Question 4 and Question 6)
- c. Investigate the possibility to test and evaluate implementations and adjust configuration of PETs in a way that fulfils their purposes. In other words, define methodologies that address the verification and the validation of privacy enhancing technologies in the automotive context. (cf. Question 3)
- d. Investigate the necessary knowledge and skills for all stakeholders involved in the software and product development life cycle. (cf. Question 3)
- e. Conduct user studies on privacy expectations and behaviours specifically in the automotive space, taking into account cultural differences. (cf. Question 5)
- f. Utilize HMI in vehicles for information and awareness on data processing and consent requests with regard to the specific situation of the driver (and passengers) in the vehicle. This may need new ideas for HMI. (cf. Question 5 and Question 6)

References

- 1 5GAA Automotive Association. *Privacy by Design Aspects of C-V2X*, 2020. https://5gaa.org/wp-content/uploads/2020/11/5GAA_White-Paper_Privacy_by_Design_V2X.pdf
- 2 European Data Protection Board. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, 2020. https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf
- 3 Jaap-Henk Hoepman. *Privacy Design Strategies*. *CoRR*, vol. abs/1210.6621, 2012.

- 4 Privacy Patterns (website). <https://privacypatterns.org/>
- 5 Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. *Tales from the dark side: privacy dark strategies and privacy dark patterns*. *Proc. Priv. Enhancing Technol.*, 2016(4):237–254, 2016.
- 6 Dark Privacy Patterns dark.privacypatterns.eu/
- 7 Gonzalo Munilla Garrido, Kaja Schmidt, Christopher Harth-Kitzerow, Johannes Klepsch, Andre Luckow, and Florian Matthes. *Exploring privacy-enhancing technologies in the automotive value chain*. In *2021 IEEE International Conference on Big Data (Big Data)*. IEEE, dec 2021. <https://arxiv.org/pdf/2209.05085.pdf>
- 8 Ezzini, S., Berrada, I. & Ghogho, M. Who is behind the wheel? Driver identification and fingerprinting. *J Big Data* 5, 9 (2018). <https://doi.org/10.1186/s40537-018-0118-7>
- 9 Sascha Löbner, Frédéric Tronnier, Sebastian Pape and Kai Rannenberg. *Comparison of De-Identification Techniques for Privacy Preserving Data Analysis in Vehicular Data Sharing*. In *CSCS '21: ACM Computer Science in Cars Symposium, Ingolstadt, Germany, November 30th, 2021*.
- 10 Blagovesta Kostova, Seda Gürses, and Carmela Troncoso. *Privacy engineering meets software engineering. On the challenges of engineering privacy by design*, 2020. <https://arxiv.org/pdf/2007.08613.pdf>
- 11 Jaap-Henk Hoepman. *Privacy Design Strategies (The Little Blue Book)* <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>
- 12 Privacy4Cars, Inc. *Vehicle Privacy Report* <https://vehicleprivacyreport.com>
- 13 <https://linddun.org/>
- 14 The European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them* https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf
- 15 <https://privacyscore.org/>
- 16 U.S. Department of Transportation. *Security Credential Management System (SCMS)* <https://www.its.dot.gov/resources/scms.htm>
- 17 Gürses, Seda and Troncoso, Carmela and Diaz, Claudia *Engineering privacy by design reloaded* Amsterdam Privacy Conference, 2015
- 18 Ala'a Al-Momani, Frank Kargl, Robert Schmidt, Antonio Kung, Christoph Bösch. *A Privacy-Aware V-Model for Software Development*. IEEE Security and Privacy Workshops (SPW), 2019.
- 19 Ala'a Al-Momani, Frank Kargl, Robert Schmidt, Antonio Kung, Christoph Bösch. *Poster: Towards A Reliable Privacy-Enhanced V-Model For Software Development*. IEEE Security and Privacy (SP), 2019.
- 20 Gürses, S., & Van Hoboken, J. *Privacy after the Agile Turn*. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (Cambridge Law Handbooks, pp. 579-601). Cambridge: Cambridge University Press, 2018.
- 21 Carmela Troncoso. *Privacy technologies need to go to the gym: on the challenges of privacy engineering in an Agile world*. Keynote at IWPE19. San Francisco, US. May 2019.

4.4 Interplay between Privacy and Trust

Thanassis Giannetsos (UBITECH Ltd., GR)

Frank Kargl (Universität Ulm, DE)

Ioannis Krontiris (Huawei Technologies – München, DE)

Francesca Bassi (IRT SystemX – Palaiseau, FR)

Anje Gering (Volkswagen AG – Wolfsburg, DE)

License © Creative Commons BY 4.0 International license

© Thanassis Giannetsos, Frank Kargl, Ioannis Krontiris, Francesca Bassi, Anje Gering

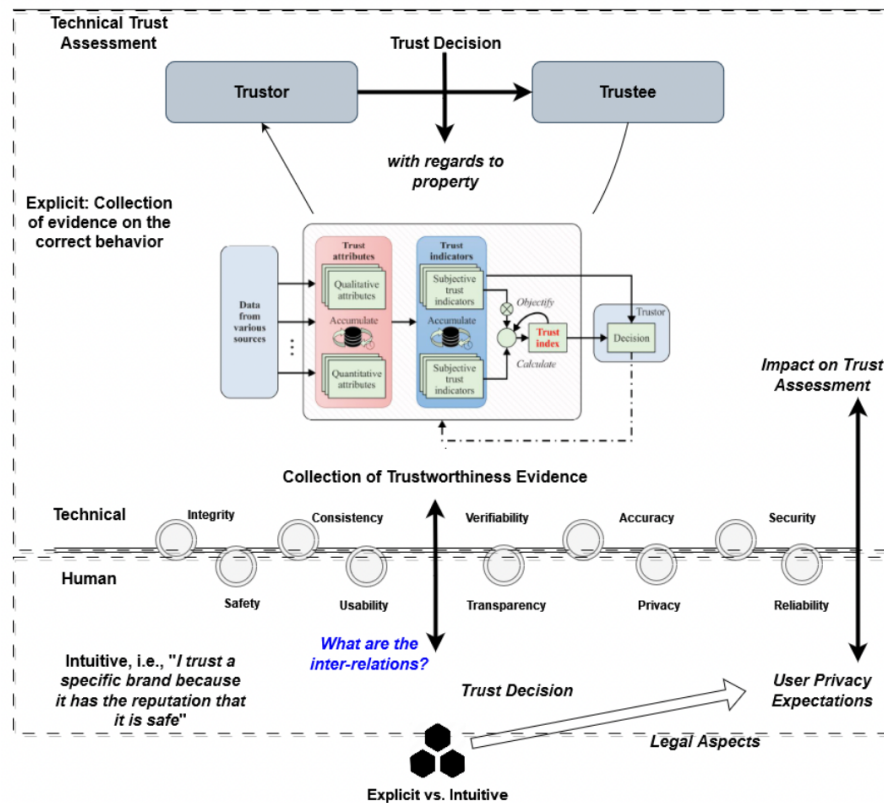
The participants of the Dagstuhl Seminar recognized the challenge of converging privacy protection of vehicle data with the need to establish trust amongst the involved actors. For that reason, a dedicated Working Group was formed with the goal to dive deeper into the interplay between privacy and trust.

Privacy and trust concerns are of utmost importance in the CCAM field, particularly with respect to vehicles and all other road users (specifically vulnerable road users). Standardized protocols, like the vehicular PKI, that function as base for establishing trust in V2X communication have effectively addressed the privacy-respecting identity management of vehicles, incorporating measures such as digital certificates and robust authentication mechanisms. Nevertheless, the issue goes beyond the mere tracing of cars and encompasses the privacy and trust implications arising from a broader set of data and the interactions between all actors (vehicles, roadside users, MEC infrastructure, etc.).

Broadly speaking, a trust relationship is a directional relationship between two trust objects that can be called trustor and a trustee. The trustor is the “source” trust object as part of a trust relationship for which trust is assessed (one who trusts, the “thinking entity”, the assessor). The trustee is a “sink” trust object as part of a trust relationship for which trust is assessed (one who is trusted). Trustworthiness then can be defined as the measure of the likelihood of the trustee to fulfill the expectations of the trustor in a given context. One way to evaluate this likelihood is by assessing whether the trustee exhibits the right and relevant set of properties that enable it to meet the trustor’s expectations in a given trust relationship. For example, consider a trust relationship between a zonal controller within a vehicle and a camera ECU during a Cooperative Adaptive Cruise Control (CACC) function where the zonal controller is a trustor that relies on the camera ECU, the trustee, to deliver non-compromised camera data to it. Here, the camera ECU needs to exhibit, among others, the property of reliability. So, assessing whether the camera ECU is reliable in passing on its data to the ECU can give positive evidence of its trustworthiness.

An indicative set of properties that are relevant for evaluation of trustworthiness of systems in C-ITS and their components can be found in sources such as documentation on standards (such as ISO/IEC TS 5723:2022, ISO/IEC 22624:2020 and Recommendation ITU-T Y.3057), existing literature on autonomous vehicle systems and trustworthiness (such as [1]), and existing documentation on CCAM (Cooperative, Connected and Automated Mobility [2]). EU Project CONNECT [3] has processed these sources and came up with a elaborated list in Deliverable D2.1, focusing specifically on the CCAM domain.

Figure 1 illustrates a list of trustworthiness properties used to evaluate a trust relationship between a Trustor and a Trustee. During the discussions, the group elaborated on those properties and categorized them in three broad categories: based on performance, based on ethical aspects and based on user acceptance.



■ **Figure 1** Assessing trustworthiness based on different evidence.

4.4.1 Trust Assessment Based on Performance

Trust and trustworthiness will play an increasingly important role as we shift towards higher levels of automation, because we need to rely on external data to facilitate partially automated or fully automated driving functions. In this context, the integrity and trustworthiness of external data sources, such as external sensor information, maps, and positioning data, becomes paramount. If the integrity of this data is compromised or not provided with the expected quality, the building blocks of the automated operation functions will use incorrect data to control the vehicle. There is a broad set of security attacks that have consequences on the trustworthiness of the data and data sources. The dependability and resilience of CCAM systems can be seriously affected by these attacks at run-time. Furthermore, there are many sources and reasons that can negatively impact dependability and safety that are not related to security. Properties like reliability, accuracy, and robustness are critical for providing consistent and dependable performance, while a property like resilience is essential for adaptability to various real-world scenarios, fostering user trust.

The issue of trust in CCAM extends beyond the realm of data and data sources. ETSI introduced the term Multi-access Edge Computing (MEC) [4] with the goal to bring processing power near the vehicle to meet ultra-low-latency requirements, and to reduce network traffic towards a centralized data-center. However, it is essential to acknowledge that such Edge Computing environments possess inherent characteristics of a complex and highly heterogeneous ecosystem due to the involvement of multiple vendors, suppliers, and stakeholders. In this context, several entities that belong to different trust domains must

interact with each other to exchange privacy-sensitive data in order to enable safety-critical collaborative services. However, if these interactions are not properly managed, it can be the cause of privacy leaks. 5GAA published a report recently describing an in-depth analysis of the trust related threats of MEC in the automotive context [5].

EU Project CONNECT [2] addresses the above challenges by building a trust assessment framework for CCAM, which can measure and manage levels of trust under uncertainty, based on incomplete and/or subjective information provided by potentially untrustworthy sources. Furthermore, this framework can accommodate dynamically changing trust relationships due to the high level of mobility exhibited during the operational time of the systems at run-time.

4.4.2 Trust Assessment Based on Ethical Aspects

Ethics-based properties are of paramount importance when considering trustworthiness due to their direct impact on public perception and societal implications. For example, the trustworthiness property of accountability emphasizes the importance of data controllers and processors taking responsibility for their actions in managing personal data. This aligns with the ethical principle of accountability, which is key in building trust as it shows that an organization is willing to be answerable for its data practices. Similarly, privacy principles require organizations to be transparent about their data practices, including data collection, processing, and sharing. When individuals can easily understand and access information about how their data is used, it fosters trust in the organization's integrity. Explainability ensures that system actions are interpretable to users and regulators, addressing concerns about the "black-box" nature of AI (or components based on AI-based technologies).

In summary, adhering to privacy and data protection principles helps organizations demonstrate ethical behavior in their data handling practices, ultimately leading to increased trust from individuals and stakeholders. By upholding strong ethical principles, CCAM systems can build a foundation of trust with users and society, promoting widespread adoption and contributing to the safe and responsible advancement of autonomous mobility technologies.

4.4.3 Trust Assessment Based on User Acceptance

When discussing the notion of trust in CCAM, we cannot ignore the dimension of human trust from the side of the passenger that will eventually make use of the AV. In that respect, trust of people to the technology is a factor directly affecting the acceptance and adoption of AVs. Research has already demonstrated that the level of trust influences the acceptance of AVs [6].

One compelling interpretation of trust revolves around the sense of vulnerability experienced by individuals inside a vehicle due to the loss of control. In that sense, trust is defined as "the extent to which drivers willingly become vulnerable when using an AV" [7]. Another interpretation of trust is from the perspective of the existence of functionality, i.e. the degree of confidence drivers and passengers have in the predictability and functionality of the vehicle [8].

In order to better understand the human aspect of trust, Kenesei et al. [9] break down trust into three categories as follows: i) trust in the performance of the AV, ii) trust in the manufacturers of the AV, and iii) trust in the institutions responsible for regulating AVs. These dimensions of trust have been elaborated in previous research as well. Eiser et al. [10] point out that people might reject an innovation even if the technology is trustworthy, simply because the organisations behind the technology are not themselves considered as

trustworthy. Liu et al. [11] adds another aspect to this dimension, raising the aspect of trust in jurisdiction. Hence, the concept of competence goes beyond mere ability, as it also includes the element of trust in governmental bodies tasked with formulating and implementing laws and regulations that assess the proficiency of these companies. These regulatory authorities grant certificates to brands that exhibit consistent adherence to the specified regulations. For instance, individuals can readily determine the extent to which different businesses adhere to the GDPR, highlighting the importance of proficiency and adherence to regulations as crucial factors in establishing confidence in the domain of data protection and adoption of technology.

Kenesei et al. [9] also explore the intricate interplay between trust and perceived risk. Indeed, when using an AV, the user should have sufficient trust that reduces the perceived risk of potential failure and misuse. More specifically, the authors examine two dimensions of risk: i) the perceived risk of the performance and hence security of the AV, and ii) the risk of misuse of the personal data that is exposed during use, which intersects with privacy protection considerations. Interestingly, their results indicate that privacy risk is influenced by trust in OEMs: trust in the manufacturer decreases the perceived risk of incorrect data handling.

In this light, it becomes evident that the policies governing how OEMs manage and process the collected data, should be considered. At the same time, the societal dimension, intricately linked to user acceptance, assumes a pivotal role in shaping trust perceptions. It becomes apparent though that the policy-making and the societal factors are intertwined, characterized by strong interdependencies that warrant thorough investigation. It is imperative to comprehend how these intertwined factors can influence users' perceived trust, and consequently, their acceptance of emerging technologies.

References

- 1 European Commission, Joint Research Centre, Fernández Llorca, D., Gómez, E., Trustworthy autonomous vehicles – Assessment criteria for trustworthy AI in the autonomous driving domain, Publications Office of the European Union, 2021, <https://data.europa.eu/doi/10.2760/120385>
- 2 European Commission, Cooperative, connected and automated mobility (CCAM), [ONLINE] https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/cooperative-connected-and-automated-mobility-ccam_en
- 3 EU Project “CONNECT: Continuous and Efficient Cooperative Trust Management for Resilient CCAM”, [ONLINE] <https://horizon-connect.eu/>
- 4 ETSI MEC ISG, “Multi-access Edge Computing (MEC); Framework and Reference Architecture,” ETSI GS MEC 003 V2.1.1, January 2019
- 5 5GAA Automotive Association. *Cybersecurity for Edge Computing*, 2023. <https://5gaa.org/content/uploads/2023/04/gmec4auto-cybersecurity-for-edge-computing.pdf>
- 6 Shariff, A., Bonnefon, JF., Rahwan, I. Psychological roadblocks to the adoption of self-driving vehicles. *Nat Hum Behav* 1, 694–696 (2017), <https://doi.org/10.1038/s41562-017-0202-6>.
- 7 S. S. Man, W. Xiong, F. Chang and A. H. S. Chan, “Critical Factors Influencing Acceptance of Automated Vehicles by Hong Kong Drivers,” in *IEEE Access*, vol. 8, pp. 109845–109856, 2020, <https://doi.org/10.1109/ACCESS.2020.3001929>.
- 8 Bernd Herrenkind, Alfred Benedikt Brendel, Ilja Nastjuk, Maike Greve, Lutz M. Kolbe, Investigating end-user acceptance of autonomous electric buses to accelerate diffusion, *Transportation Research Part D: Transport and Environment*, Volume 74, 2019.

- 9 Zsófia Kenesei, Katalin Ásványi, László Kökény, Melinda Jászberényi, Márk Miskolczi, Tamás Gyulavári, Jhanghiz Syahrivar, Trust and perceived risk: How different manifestations affect the adoption of autonomous vehicles, *Transportation Research Part A: Policy and Practice*, Volume 164, 2022, <https://doi.org/10.1016/j.tra.2022.08.022>.
- 10 Eiser, J. R., Miles, S., Frewer, L. J. (2002). Trust, perceived risk, and attitudes toward food technologies. *Journal of Applied Social Psychology*, 32(11), 2423–2433.
- 11 Peng Liu, Zhigang Xu, Xiangmo Zhao, Road tests of self-driving vehicles: Affective and cognitive pathways in acceptance formation, *Transportation Research Part A: Policy and Practice*, Volume 124, 2019,

Participants

- Ala'a Al-Momani
Ulm University, DE
- David Balenson
USC Information Sciences
Institute – Marina del Rey, US
- Francesca Bassi
IRT SystemX – Palaiseau, FR
- Christoph Bösch
Robert Bosch GmbH –
Renningen, DE
- Benedikt Brecht
Volkswagen AG – Berlin, DE
- Michael Buchholz
Universität Ulm, DE
- Stefan Gehrler
Robert Bosch LLC –
Pittsburgh, US
- Anje Gering
Volkswagen AG – Wolfsburg, DE
- Thanassis Giannetsos
UBITECH Ltd. – Athens, GR
- Kevin Gomez
TH Ingolstadt, DE
- Kyusuk Han
Technology Innovation Institute –
Abu Dhabi, AE
- Adam Henschke
University of Twente, NL
- Mario Hoffmann
ARRK Engineering GmbH, DE
- Frank Kargl
Universität Ulm, DE
- Ioannis Krontiris
Huawei Technologies –
München, DE
- Brigitte Lonc
Nanterre, FR
- Zoltán Mann
University of Amsterdam, NL
- Jason Millar
University of Ottawa, CA
- Christos Papadopoulos
University of Memphis, US
- Sebastian Pape
Continental Automotive
Technologies – Frankfurt, DE
- Jonathan Petit
Qualcomm, US
- Sarah Thornton
Nuro – Mountain View, US
- Natasa Trkulja
Universität Ulm, DE
- Bryant Walker Smith
University of South Carolina –
Columbia, US
- Takahito Yoshizawa
KU Leuven, BE

