The road to connected vehicles

Privacy and security concerns in the next era of transportation

Adrian Bjugård
Chalmers University of Technology
bjugard@student.chalmers.se

Kim Kling
Chalmers University of Technology
kkim@student.chalmers.se

Pontus Malm
Chalmers University of Technology
malmpo@student.chalmers.se

ABSTRACT

The next generation of vehicles will be connected, not only to other vehicles but to the Internet and to their respective manufacturers as well. Collecting data from such connected vehicles has many use cases and provides useful information and insight for both manufacturers and consumers. This collection of information can have a negative impact on consumer privacy, since their habits and otherwise private information is recorded and processed by an external actor. The manufacturers responsible for data mining operations need to make sure to minimise their impact on consumer privacy. Ultimately, in order for the consumers to accept being a part of this data mining, they need to feel that the benefits outweigh the downsides.

Connectivity in vehicles also introduces new concerns for vehicle safety, as adversaries are provided a new way to attack vehicles remotely. Security is especially important in connected vehicles, as if an adversary gets in it has the potential to cause damage to real world objects or in worst case, lives.

This survey investigates the possibilities of handling the privacy and security concerns for consumers while still reaping the benefits of connectivity. Algorithms can be used to mask sensitive and private information, making it indistinguishable among the collected data. The survey will also evaluate the usefulness of the anonymised data and investigate if the masked information is truly anonymous. Security practises and algorithms used to limit distant entities in communication are introduced.

We present several algorithms that enable some anonymisation of consumer data, but also removes some of the benefits for the collector. The survey concludes that there is a fine line where privacy and benefits meet, that this line is set by the consumers, based on how they are rewarded for providing information about their usage. There is no obvious way to handle this, but to always motivate and be transparent about what is gathered and why.

Keywords

Privacy, security, connected vehicles

1. INTRODUCTION

We live in a connected world where the advantages of connecting things is massive. They can assist the user with help from other users, and report usage info in order for a manufacturer to improve its product or service. But with all these advantages, it is important to remember the privacy and security of the users' data in a world of connected devices.

Vehicles are prominent devices that increasingly utilise connectivity in order to improve safety, reliability, efficiency, and usability. In the case of connected vehicles it can provide the manufacturer with information about how the vehicle is used, in order to improve future models. Another feature that benefits the user is communication between cars. Such features can be used to report hazards, accidents, and dangerous traffic conditions from one vehicle to another. This improves how the user utilises the vehicle, but could also be used to maliciously affect a vehicle.

This survey summarises the challenge of maintaining privacy and security for data in a connected vehicle. An evaluation of different methods to maintain privacy with regards to data sent away from the vehicle is within the scope, as well as the security implications of such systems. It does not address privacy or security concerns for communication within a vehicle.

The survey is organised as follows. Section 2 introduces some background, describing how as well as why vehicle manufacturers integrate connectivity in their vehicles and describes what it is used for in such vehicles. It also defines privacy and security in the context of connected vehicles. Section 3 surveys a set of algorithms used to maintain privacy. Section 4 surveys a set of methods to maintain a high level of security while introducing connectivity to vehicles. Section 5 discusses the surveyed solutions with respect to the level of privacy they provide, and the amount of useful data the requester still gets. It also discusses how security is achieved without limiting the services provided. In the end of this survey, Section 6 concludes the survey.

2. BACKGROUND

This section provides some background and explains the core concepts that are relevant to the survey. A baseline is laid out for information about connected vehicles, privacy and security.

2.1 Connected Vehicles

A connected vehicle has a single feature that distinguishes it from traditional non-connected vehicles. It has, and uses, an ability to communicate with entities outside of the car. These can be peers in an ad-hoc network such as other vehicles, traffic signs, roads or data collectors such as a manufacturer, or insurance company. The type of communication is separated into two categories; Vehicle-to-Everything (V2X) communication and service provider communication.

V2X is a category for the types of communication used to communicate between a vehicle and something else that is in close proximity to the road. In this group of communication types, we find Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and more. This category of communication is mainly used to improve safety for travellers and pedestrians. It enables the different entities to send and receive information such as their speed, braking, road conditions, and upcoming hazards. [Glancy, 2012]

While this communication is used in order to improve safety for all parties, a malicious user can chose to send malicious data in order to confuse or trick another party into making a bad decision. This falls under the bogus information attack [Tyagi and Dembla, 2014]. Therefore we need to, if possible, verify the information and decide whether we can trust it or not. There should be no assumption that information received from any V2X node is valid or secure. When sending information via V2X, we also need to decide what level of privacy we want to achieve. In order to provide useful V2X data, some privacy sensitive information may be required to be provided in order for the system to be useful.

Many systems use Vehicular Ad-hoc Network (VANet) which is a network that enables vehicles to utilise V2X communication via a dedicated network. This allows vehicles to inform others and retrieve information about current speed, position, road conditions, as well as other potential road hazards. [Glancy, 2012; Tyagi and Dembla, 2014]

Communication with any party that is not covered by V2X communication is in this survey called service provider communication. This communication is subject to attacks, just like any other kind of network. Regarding privacy, the user must stay cautious about what information is provided to a service provider.

2.2 Privacy

In order to more effectively be able to discuss the subject of privacy, as it pertains to the collection of personal data in connected vehicles, we must first establish some definitions and background on the related subjects.

2.2.1 Definition of Privacy

"Privacy" is a subject though which many new technologies, particularly those with elements of surveillance, are often critiqued [Lyon, 2003]. However, as a concept, privacy is difficult to define. According to S. Gutwirth "The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as 'our' privacy, it still finds a way to remain elusive" [Gutwirth, 2002]. Nissenbaum argues that privacy is best described through the notion of "contextual integrity". That it is not the initial sharing of information that is the problem, but rather the subsequent sharing of information outside of socially agreed contextual boundaries [Nissenbaue, 2004]. Since many new advancements in connected vehicles require personal information to function, we are forced to disclose certain information if we want to use those features, or at times, if we want to use modern vehicles at all.

Finn et al. separates privacy into the following seven different categories: privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy) [Finn et al., 2013].

These privacy categories can be related to connected vehicles through the vehicles various sensors. For example, privacy of the person can be violated by disclosing results from breathalyser hardware. Privacy of personal communication by utilising off-site analysis tools on voice recordings provided by microphones in the vehicle. Privacy of location and space by disclosing GPS coordinates. Privacy of behaviour and action by analysing patterns in aforementioned GPS coordinate data, among others.

2.2.2 Privacy in the Modern Era

Privacy is of varying importance to different people, but most have some aspect of their lives that they prefer to keep private. Beginning with the introduction of the Internet in the late 1980s, over time communication, and more generally the spreading of information, has become increasingly more available. From our computers all the way to household objects like light bulbs, the amount of Internet-connected devices with sensors capable of divulging potentially private information is growing rapidly. Maintaining one's privacy is harder than it ever has been before as a result of this growth.

2.2.3 Money in Exchange for Limited Privacy

Companies involved with product development, insurance, and advertising are a few of the actors who stand to benefit economically from increasing their access to personal information. Since consumers place value in keeping such information private, gaining access to it is met with resistance unless the consumer feels they are gaining something by providing it. As such these actors need some way of assigning an acceptable value to different types of information, in order to be able to properly compensate consumers.

In their 2015 paper on the subject, Derikx et al. investigated whether and how privacy concerns of vehicle owners can be compensated by offering monetary benefits based on flat rate values of different categories of privacy-infringing information [Derikx et al., 2015]. They concluded that depending on who the recipient of the data is, people are more or less willing to divulge private information in exchange for some form of economic compensation. Advertising agents were found to be the least appealing for consumers to share their information with.

2.2.4 Data Leaving the Vehicle

Most high end vehicles manufactured in recent years have a myriad of sensors. Whether it is a simple seatbelt sensor, a GPS sensor, a microphone, or a reversing camera, the vehicle has the ability to record data from all of these sensors.

In order to provide a requested service, recorded data is sometimes relayed to the vehicle or system manufacturer and its partners, via Internet-connected systems like Volvos OnCall, Volkswagens Car-Net, and General Motors OnStar. This allows the manufacturers to perform vehicle diagnostics remotely, but requires some data to be transmitted from the vehicle in order to do so.

Besides transmitting data to the vehicle manufacturer via Internet-connected systems, the IEEE has developed a standard for V2V communication called 802.11p [Jiang and Delgrossi, 2008]. This technology has the potential for allowing malicious entities to read and store data about the habits of road users without their knowledge.

2.3 Security

The security of a system depends on several factors and can be asserted using different metrics. In this section a baseline for security in the context of connected vehicles is established.

2.3.1 Definition of Security

Security, in the context of information technology, is defined as "the protection of information against being stolen or used wrongly or illegally" [Cambridge University Press, 2016]. In practice, security is a term that describes how resistant something is to attacks by an adversary. A common model to assert security is the CIA Triad model which takes three properties into account; Confidentiality, Integrity and Availability [Kleberger et al., 2011; Plößl and Federrath, 2008].

In our increasingly digital world, security is highly demanded in connected systems. No matter the importance of the system itself, consumers want to feel that they are the ones in control of their connected systems.

2.3.2 Security in Connected Vehicles

Digital systems in vehicles have existed for a long time, often interconnected through an internal communications network known as a Controller Area Network (CAN) bus [Johansson et al., 2005]. But since traditional vehicles have not been connected to external networks, potential security issues were accessible only through direct contact with the vehicle. This is because the aforementioned CAN-bus is, in such vehicles, not exposed outside the vehicle. Connecting any system to the Internet makes it a potential target for network-based attacks against it. Either via directly targeted attacks, or via automated attacks scanning through a network for devices to attack. Since the modern connected vehicle is often connected to many external service providers via the Internet, securing the external communication becomes a necessity to assert the safety of the vehicle.

2.3.3 Attacks on Connected Vehicles

Several attacks are possible on a connected vehicle. Tyagi et al. defines a taxonomy to describe several attacks on communication between vehicles that uses the VANet [Tyagi and Dembla, 2014].

Attacks can be categorised as being either passive or active. Passive attacks are undetectable by a user, and among them we find eavesdropping, location disclosure, and traffic analysis. The active attacks are malicious packet dropping and routing. Routing attacks are in turn divided into five categories; sleep deprivation, black hole, grey hole, rushing, as well as the Sybil attack. [Tyagi and Dembla, 2014]

These attacks affects a superset of properties in the CIA model. Besides Confidentiality, Integrity and Availability, Tyagi et al. highlights more attributes that are important in the context of connected vehicles. Among these are Authentication and Non-repudiation.

Authentication enables the messages in the VANet to be limited to affected nodes, either by distance or by authenticate individual nodes. Non-repudiation enables the ability of always being able to prove that a sender sent a message, even in the event that a sender tries to remove traces from their node.

As previously mentioned, communication with a service provider is often routed over the public Internet and enables general network attacks on the traffic.

3. PRIVACY SOLUTIONS

The collection of data from connected vehicles can provide useful information for both consumers and the manufacturers as mentioned in the introduction. All data from the sensors in a vehicle, as well as the internal communication, can potentially be collected and uploaded to its manufacturer. This gathered information can potentially infringe on consumer privacy. Giving the user control and using technical abilities to care for the privacy, users' interests can remain respected within the industry.

3.1 Advantages of Data Mining

There are many advantages to data mining. For example, the user can take part of location based services by sharing their geolocation data. A connected vehicle that needs to refuel can then provide its driver the location of the closest gas station. A manufacturer can potentially use data collected from sensors to understand a vehicles immediate surrounding. Such data can then be used to discover temporary road obstacles or monitor traffic [Future of Privacy Forum, 2014]. Insurance providers can use the collected data to provide personalised insurance quotes to customers. As the insurance provider can better assess its own risk associated with a certain customer, it can provide cheaper insurance to lower risk customers.

3.2 Privacy Algorithms

Data utility and privacy are two conflicting goals when collecting information. By retrieving and storing data as is, there is no guarantee of privacy. If the goal is to provide good privacy the usefulness of the collected data may be limited. The thesis, *Models and Algorithms for data privacy*, categorises algorithms for protecting privacy in statistical databases into two frameworks, the interactive and the non-interactive frameworks [Kenthapadi, 2006].

3.2.1 Interactive Framework

The interactive framework queries the database through a privacy mechanism that can either deny or alter the query to ensure privacy. One of the two main methods that can be used in the interactive framework is query auditing. It simply denies queries that can reveal sensitive information according to the databases specified disclosure policies. The other method that can be used by the privacy mechanism is output perturbation. This method computes the exact answer to a query but adds some noise to the data to provide privacy. The extra noise has the drawback of returning false information.

3.2.2 Non-interactive Framework

The non-interactive framework stores data in a modified form to ensure privacy. Information can be accessed directly from the database. There are several privacy methods in this category. Noise can be added to the data as input perturbation similar to the method in the interactive framework to mask identifying data. The concept of k-anonymity can be an important tool for ensuring privacy in sets of data. It is a property for avoiding record linkage by grouping data in such a way that every possible query to the database will return a result based on at least k records. The variable k acts as a parameter for the privacy of the database. For

higher values of k, the available parameters for the queries becomes more restricted and will therefore result in more limited information. [Samarati and Sweeney, 1998]

3.3 Re-identification From Anonymised Data

While not strictly containing information identifying a certain user, some data that is collected may by its very nature be used to profile and identify a specific individual. Without including any other data, GPS location combined with a timestamp can be used to figure out where the vehicle owner lives, the driving patterns, where they work, where they shop, to name a few, breaching privacy of location and space. Alcolock systems can show whether the driver is often near the legal limit, breaching privacy of the person. Nothing prevents the built-in microphones inside a vehicle from being activated without user consent, breaching privacy of communication as well as privacy of behaviour and action in some cases. If the GPS data does not reveal a singular driver, but for instance, that the driver lives in a home where there are multiple capable drivers, then one can look at seat or mirror positions for example, in order to identify the specific driver. In some modern vehicles, the seat and mirrors are even automatically adjusted based on which key is used to unlock a vehicle. Seat sensors may also reveal whether there is a passenger in the vehicle, which may in some instances be considered private information.

Clearly there is a lot of data which seems innocent to report, but reveals a lot when pieced together with other innocuous pieces of information. One potential method of anonymising this type of data is to make it impossible to link it to the other data points reported from the same vehicle, instead bundling it with the same data from many other vehicles, perhaps even from different manufacturers or model series. This is a controversial solution since, as discussed in Section 3.2, the data becomes significantly less useful when this is done.

4. SECURITY SOLUTIONS

Introducing connectivity to vehicles enables many useful features, but also opens up for potential security issues. It is a challenge to find the correct balance of risk versus reward regarding any system where security is a factor. When it comes to security in connected vehicles, the stakes are especially high and the task should be met by applying known security mechanisms and best practises.

4.1 Over the Air Firmware Update

Over the air firmware updates are a feature of many recent connected vehicles [Dakroub and Cadena, 2014]. They allow the manufacturer to install software updates to the vehicles' on-board computers without the customer having to visit a service centre. Such updates could enable new features not available at launch or patch holes in the vehicle security systems. Of particular importance is the ability to improve vehicle security as soon as vulnerabilities are discovered, as it minimises the risk that a particular vulnerability is used on a particular vehicle.

Since software updates can be performed over the air, the importance of verifying the communication with the software update distributor is increased. But due to the dynamic nature of the Internet it is not sustainable to, for example, lock communication to one specific IP address, as that could change over time, or be made inaccessible by a denial of service attack. The solution to this particular problem is to use encrypted communication with pre-defined trusted security certificates, where the vehicle only accepts connections from servers signing their communication with such a pre-determined signature.

It is important to also consider the encryption standard used as, due to advances in computational power, certain ciphers such as DES (Data Encryption Standard) can these days be broken in a matter of hours with relatively cheap hardware. The same is not true for the AES (Advanced Encryption Standard) or RSA (named after the authors Ron Rivest, Adi Shamir, and Leonard Adleman) standards when used with a sufficiently large key size.

4.2 Gateway Firewalls

Wolf et al., while discussing systems for automotive bus security, briefly mentions the notion of introducing firewalls on gateway systems in the connected vehicle [Wolf et al., 2004]. Their work focused on protecting the vehicles internal CAN-bus communication from external attacks. As connected vehicles become more complex, it becomes possible to attack higher levels of the vehicles systems, requiring more advanced packet filtering firewalls. Such a firewall, besides disabling external access to sensitive internal systems, can also serve as a means of protecting internal systems with limited processing capabilities against network flooding attacks.

4.3 Distance-Bounding Protocols

In some instances it is necessary to ignore communication originating from a large distance. This is interesting in particular in VANets where messages coming from further away are often irrelevant, and we really only want to listen to entities close by. As a solution to this, Brands et al. introduces the concept of distance-bounding protocols in their 1993 paper on the subject [Brands and Chaum, 1993]. The principle this protocol is based on is a simple measurement, essentially timing how long it takes to receive a response after sending a message. As described by Brands et al., "It consists of a single-bit challenge and rapid single-bit response. In practice, a series of these rapid bit exchanges is used, the number being indicated by a security parameter k. Each bit of the prover P is to be sent out immediately after receiving a bit from the verifier V. The delay time for responses enables V to compute an upper-bound on the distance" [Brands and Chaum, 1993].

This type of protocol allows a node to limit the number of recipients for any reasons, such as when transmitting privacy sensitive information that is only intended for nodes nearby. It can be speed and distance which, for example, may only be intended for nodes within one kilometre.

4.4 Achieving Security Properties

In order to achieve the desired security properties outlined in Section 2.3.3, we need to integrate cryptography into the protocols that communicate over VANet. This is done by signing and encrypting messages wherever appropriate. Proper authentication can be implemented by taking advantage of the public key system. Availability can be achieved by capping the traffic from a node to a maximum threshold, in order to allow non malicious traffic to be accepted.

5. DISCUSSION

The subject of connected cars introduces new discussions regarding privacy and security. There is no obvious way to handle the addition of remotely accessible systems, designed to automate and gather private information, to what is essentially quite a deadly machine in the wrong hands.

5.1 Privacy vs Value

Services that become possible by connecting vehicles to the Internet can be a key selling point, or even a requirement, as connected vehicles become more common. What consumers have to ask themselves is whether they are comfortable with giving up a certain level of privacy. As mentioned in earlier sections, different services require the sacrifice of different types of privacy. If, for example, a consumer wants to use a voice-enabled personal assistant software, their voice must be recorded and analysed off-site, there is no way around that. While the privacy trade-offs should be clear to the users deciding about them, service provider must also provide choices for privacy concerned users. The choices might limit usability with increased privacy. By enabling choices, and the ability to later change the choice, the user can take control of the level of privacy they get.

As mentioned in Section 3.3, some services require data that is by nature impossible to completely anonymise. Mapping services will not function at all if the service provider can not know the location of the user, and the location of the user together with the time is enough information to figure out where the user lives, works, shops, and eventually the identity of the user will be evident. Knowing this, users are forced to choose between using the related service or to keep their privacy intact.

5.2 Terms and Conditions Updates

The Terms and Conditions of digital systems are often very long documents describing what kind of privacy sensitive information the system gathers, as well as who that information will be shared with. But whenever that system is updated, there is often some kind of change to the Terms and Conditions that accompany it, prompting the user to agree to the same very long document again, probably before being allowed to start their vehicle or at least their vehicles infotainment system. Whether or not the user even read the document the first time around, they will be less inclined to read it again this time. This has the potential to leave the user in a situation where they are sharing some privacy sensitive information that they are not actually comfortable sharing, but did not know that the new version was sharing.

5.3 Trust

Ultimately, when sharing private data with an external actor, everything eventually comes down to trust. Do you trust that the specific actor you are sharing your data with will abide by the restrictions of your contract with them? Even if the data the service providers can access is anonymised using the mentioned algorithms for increasing privacy, it is hard for a customer to know exactly what data the vehicle is transmitting. This is a matter on which users will have differing opinions, but major incidents like the 2015 case of Volkswagen lying about their vehicles NO_X emissions represent real causes for concern about the honesty of vehicle manufacturers [Ewing, 2015]. Similarly, bad privacy or security can result in lower trust for both the manufacturer and connected vehicle technology as a whole.

5.4 An Open Network

With connectivity that utilises VANet, new types of problems occur. Compared to the Internet, where many nodes use point to point communication, a VANet node uses the connection in order to broadcast information to other nodes and to listen for broadcasts that may concern themselves. The notion of a connection is not required and the notion of transmissions is more likely.

This type of network changes how we communicate over the network and requires the use of a trust based solution for what we receive. It is absolutely crucial that everything received is verified as much as possible by integrating cryptography and by comparing the data to other sensors on the vehicle (distance sensors, measuring the round trip time etc) as well as trying to get the information verified by other nodes in the network (road hazards, accidents, etc).

Regarding privacy, there is an interest in limiting who can receive and answer to privacy sensitive information transmitted. For this problem, distance-bounding protocols are of great benefit. It enables the sender to specify different ranges for different types of information and can ensure that the ability to track is limited to being in close proximity to the node. If not secured with distance-bounding protocols, V2X communication greatly affects privacy, since malicious entities have the ability to access the system as well. They could collect data transmitted and use it to extensively map the habits of a user. They could also inject bogus data into the system, tricking nearby vehicles into thinking there is a road hazard nearby, or for example that there is already a person or vehicle in an intersection when in fact there is not, effectively stopping traffic.

5.5 Vehicles Are Computers

Modern vehicles are highly digital and contain millions of lines of code [Broy, 2006]. It is naive to believe that the code inside a vehicle is completely free from bugs, and introducing vehicles to the Internet has opened up new ways of accessing these systems. Connected vehicles are possible targets for malicious attacks just like computers. Due to the nature of certain systems in a vehicle, an attack on the security of a vehicle can have impact on the safety of the user. The need for security reviews and other tools to ensure good security is of great importance because of this. As mentioned in Section 4.1, with the connectivity of vehicles it is possible to provide security updates over the air. Since connected vehicles can patch themselves when a new update is available, vehicles will not be exposed to known vulnerabilities for a long time. Instead, they will be patched just like any computer operating system.

5.6 Autonomous Vehicles

Autonomous vehicles are vehicles that can be controlled without human input. The digital systems in such vehicles have much more control than in a traditional, non-autonomous vehicle. As such, the malicious use of an autonomous vehicle can be much more severe, as an attacker can possibly have greater access to the vehicle than the person using it.

6. CONCLUSION

By connecting vehicles to networks, regardless of it being an external service provider via the Internet, or to a VANet, new features not previously possible can be made available to users. These include everything from safety conscious features, such as systems for emergency warnings and automatic collision avoidance, to streaming music and complete platforms for installation of user applications. There are a myriad of new features made possible by the introduction of connectivity to vehicles.

While enabling new features, this connectivity can also introduce general network problems into the vehicles, which when used maliciously, can be used to cause harm to other people. If an attacker instead chooses to use this connectivity to track and map a persons life, the connected vehicle is a gold mine of information for them.

By having privacy and security as a part of the main objectives when designing the systems, users can feel confident that their lives and interests are being looked out for. Users must have the possibility to choose what level of privacy they are willing to give away, and in a transparent manner see what data different service providers and entities in the VANet have access to.

What kind of data is recorded from a vehicle must be carefully considered before any system that reports it is rolled out. Even seemingly innocuous data like the position of the driver seat and the no-seatbelt warning system for the passenger seat may in certain situations, coupled with other types of date, divulge information that some might consider private. If such data is necessary to be recorded for statistics or similar purposes, then it may be necessary to disconnect it from other data collected from the vehicle, by bundling it with data from other vehicles and as such hiding its origin.

When it comes to security, this survey has looked at solutions to some issues that are relevant to connected vehicles. Among those introduced are over-the-air software updates, firewalls, distance-bounding protocols, and encrypted communication. It is clear that these solutions are necessary steps in order to build a secure connected vehicle, but that there is still work to be done in regards to securing V2X communication.

References

S. Brands and D. Chaum. Distance-bounding protocols. *Theory and Application of Cryptographic Techniques*, pages 344–359, 1993.

M. Broy. Challenges in automotive software engineering. In *Proceedings of the 28th international conference on Software engineering*, pages 33–42. ACM, 2006.

Cambridge University Press. Meaning of security in the english dictionary. http://dictionary.cambridge.org/dictionary/english/security, 2016. (Accessed on 2016-09-22).

H. Dakroub and R. Cadena. Analysis of software update in connected vehicles. *SAE International Journal of Passenger Cars-Electronic and Electrical Systems*, 7 (2014-01-0256):411–417, 2014.

S. Derikx, M. de Reuver, and M. Kroesen. Can privacy concerns for insurance of connected cars be compensated? *Electronic Markets*, 26(1):73–81, 2015.

J. Ewing. Volkswagen says 11 million cars worldwide are affected in diesel deception. *The New York Times*, 22, 2015.

R. L. Finn, D. Wright, and M. Friedewald. Seven types of privacy. In *European data protection: coming of age*, pages 3–32. Springer, 2013.

Future of Privacy Forum. The connected car and privacy - navigating new data issues. http://fpf.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November2014.pdf, 2014. (Accessed on 2016-09-25).

D. J. Glancy. Privacy in autonomous vehicles. *Santa Clara L. Rev.*, 52:1171, 2012.

S. Gutwirth. *Privacy and the Information Age*. Critical Media Studies- Institutions, Politics, and Culture. Rowman & Littlefield Publishers, 2002. ISBN 9780742517455.

D. Jiang and L. Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040. IEEE, 2008.

K. H. Johansson, M. Törngren, and L. Nielsen. Vehicle applications of controller area network. In *Handbook of networked and embedded control systems*, pages 741–765. Springer, 2005.

K. Kenthapadi. *Models and Algorithms for data privacy*. Stanford University, 2006. URL \url{http://theory.stanford.edu/~kngk/papers/krishnaramKenthapadiThesis.pdf}.

P. Kleberger, T. Olovsson, and E. Jonsson. Security aspects of the in-vehicle network in the connected car. In *Intelligent Vehicles Symposium (IV), 2011 IEEE*, pages 528–533. IEEE, 2011.

D. Lyon. *Surveillance after september 11*, volume 11. Polity Press, in association with Blackwell Pub, 2003.

H. Nissenbaue. Privacy as contextual integrity. *Washington Law Review Association*, 79:119, 2004.

K. Plößl and H. Federrath. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Computer Standards & Interfaces*, 30(6):390–397, 2008.

P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical report, SRI International, 1998.

P. Tyagi and D. Dembla. A taxonomy of security attacks and issues in vehicular ad-hoc networks (VANETs). *International Journal of Computer Applications*, 91:22–29, 2014.

M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*, 2004.