Smart Technologies – Workshop on Challenges and Trends for Privacy in a Hyper-connected World*

Andreas Baur-Ahrens[1], Felix Bieker[2], Michael Friedewald[3], Christian Geminn[4], Marit Hansen[2], Murat Karaboga[3], Hannah Obersteller[2]

[1] Intl. Centre for Ethics in the Sciences and Humanities, University of Tübingen, Germany
a.baur-ahrens@uni-tuebingen.de
[2] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany
{fbieker|marit.hansen|hobersteller}@datenschutzzentrum.de
[3] Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, Germany
{michael.friedewald|murat.karaboga}@isi.fraunhofer.de
[4] Research Center for Information System Design, Universität Kassel, Germany
c.geminn@uni-kassel.de

Abstract. In this workshop we will address what it means to live in a smart world with particular regard to privacy. Together with the audience, we will discuss the impacts of smart devices and appliances on individuals and society as a whole. To that end, specific examples of smart devices will be addressed based on topicality.

Keywords: Smart Devices, Smart Cars, Privacy, Data Protection, Ethics. Internet of Things, Regulation

1 Motivation

Smart devices have begun to invade more and more aspects of our everyday lives. They can assist their owners while driving, while working out, while shopping and in the context of many other activities. Whereas first generation devices often lacked the refinement necessary for immediate economic success, they act as a window into the future by demonstrating the seemingly endless possibilities of a 'smart world'. Other smart devices and systems are already well established, for instance those that are concerned with assisted driving.

However, while smart cars are comparatively new to the market and still under development, the general challenges for privacy resulting from connection and interaction are not. The question arises whether and how we can learn from experiences with internet and smart phone usage with data traces, profiling of users and a lack of transparency to foster a privacy-enhancing design of smart cars and their infrastructure.

* This work is partially funded by the German Ministry of Education and Research within the project 'Forum Privacy and Self-determined Life in the Digital World'.

D. Aspinall et al. (Eds.): Privacy and Identity 2015, IFIP AICT 476, pp. 111–128, 2016.
DOI: 10.1007/978-3-319-41763-9_8

From a legal perspective, the increasing quantity and quality of smart devices and appliances is foremost a challenge to the right to respect for private and family life as well as the right to protection of personal data as established in the Charter of Fundamental Rights of the European Union. Furthermore, national basic rights like Germany's right to informational self-determination come into play.

From an ethical point of view, a world where decisions are increasingly influenced – or even made – by smart and data gathering devices raises an array of questions. For instance, which opportunities for action do we value as crucial for human beings and how much control do we give to technologies and technical systems? One way of addressing these questions is to look at structural and diffuse power relations that govern the field. This is not only related to power of smart technologies themselves, but also to social actors' power enhanced by smart devices and the power of concepts, e.g. 'efficiency' that might oppose values like individual privacy. A relatively broad concept of power can help to evaluate the impact of a world of smart appliances.

The challenges that smart devices entail for privacy in modern societies necessitate solutions that are aimed at providing a reasonable balance between the interests of users, state actors and economic players on the hand and on a more generic level between socially desirable and unacceptable technological upheavals. With reference to the aforementioned legal and ethical perspectives, a political science point of view deals with the question, which particular regulatory measures (e.g. hard regulation, co-regulation, self-regulation) are to be taken into consideration in order to shape the digital future in a socially appropriate and sustainable manner.

2 Workshop Content

The workshop began with a short introduction by the organizers, giving a broad overview of the topic, namely of more general challenges and trends resulting from current technological developments in the field of smart devices. The different disciplines and perspectives involved in the workshop – namely technology and law, as well as social and political sciences – were highlighted.

2.1 Privacy Risks for Smart Car Users – Lessons Learned from Internet and Smart Phone Usage

The introduction was followed by the first presentation, entitled *Privacy Risks for Smart Car Users – Lessons Learned from Internet and Smart Phone Usage*. [1], [2]

Focusing on the technical background and consequences for the user who is faced with smart devices, and thereby outlining the issues from a technical and data protection perspective, the presentation also served as a general introduction to the issues raised by the following talks. Starting point was a comparison of upcoming smart cars with – already well-established – smart phones. It was argued that – from a technical point of view – the same issues occur (again). Consequently, now that the number of smart cars increases and a strategy for handling upcoming issues has to be found, it is recommended to take a look back to earlier developments and learn from shortcom-

ings, close gaps, and thereby create a framework which allows to profit from the technical progress, but respects the rights of the individuals. Here, three main aspects have to be considered: Internet and telecommunication is used for functionalities provided in the car, information from and about the car is not only locally processed, but also in the external communication networks or even in clouds, and finally, the car and its components have to be regarded as network nodes.

"Smart cars", respectively every single componenkt which makes the car a smart one, gather manifold kind of data from manifold sources. Most of it is to be considered as personal data and as such falls under the data protection legislation. The data is collected by several sensors, transmitted with different techniques and potentially stored and exploited in multiple ways. In "smart cars", especially the following data concerning the vehicle is accumulated and accessible via the OBD-II-port: the Unique Mobile Device Identifiers all mobile devices have, the numbers of SIM cards used for transfer of data e.g. needed for voice controlled components (such as navigation assistance), MAC addresses of those network components needed to connect with WiFi hotspots, Bluetooth identifiers as far as Bluetooth is employed to connect e.g. a smart phone, RFID identifiers as they are needed for key remote controls. Whenever the respective devices, or: components, on board communicate with the external world, this data is transferred as well. Furthermore, information on the device setting (e.g. language) is communicated. In total, this "phenomenon" is not new, but very similar to the functioning of internet browsers.

Now, in addition to these issues already known from former technological achievements, smart cars are equipped with multiple sensors, measuring the status of "classical" car components. This means, data on e.g. tire pressure, engine and gear, as well as breaks is collected and possible error messages are stored. Also, in most modern cars GPS transmitter are installed. They allow to collecting data on the exact position of a car, the direction it is going and the current, and generally deliver more precise results than (just) tracking the vehicle via speed mobile radio cells and WiFi hotspots [3]. Besides data of the smart car, also data directly related to the driver and/or passengers is collected: The driver maybe to create a user account first in order to make use of the smart components of the car. For this purpose, personal data like name and address has to be indicated. The smart car is able to store different preferred settings (from side mirrors to infotainment), for different drivers. Also, biometric data can be used to identify the driver as authorized to drive the car. Finally, some systems are monitoring and analyzing medical data of the driver (e.g. heartbeat or eye movement) in order to e.g. find signs of fatigue.

All this data is collected and can be extracted from the smart car. Yet, another parallel to former technological developments: Unsurprisingly, many business models to use this data in a meaningful way already exist or are under development. As examples serve car insurance companies who offer insurance policies following the "pay as you drive" model. This means, all car data is analyzed by the insurance company and the individual insurance rate is calculated accordingly.

Another example is the "expansion" of big mobile phone or IT companies to the automobile sector (mainly with the goal to integrate their system software into the car and facilitate a connection to their mobile devices) [4]. Just like the internet user data,

now also the driver data can be analyzed to offer more personalized and more specific services like e.g. personalized maps or navigation services. Those are able to take into account personal habits of the driver. This means, for instance, the driver can choose not to drive routes which pass casinos. All this data needs to be transferred to the service providers. This creates "usage patterns" as they are known from internet usage. Data footprints allow identifying and tracking the driver. Furthermore, due to the enormous volume of data that is collected and of course for practical reasons, the smart car data is often stored in clouds. This raises the question how it can be guaranteed that every data is only used for the purpose it was collected for, not merged or aggregated beyond this dedication and not accessed by an arbitrary amount of parties. As shown above, this driver data is potentially even different quality of personal data and therefore – especially in combination with the personal settings – can be used to create very precise profiles of the drivers. This makes the question of secure storage and access to those profiles even more delicate. Of course these issues are known from established online services. With respect to the developing market of smart cars, history should not (completely) repeat itself. Research on data-minimising techniques and methods for use in smart cars is ongoing. Although interesting approaches, such as frequent change of pseudonyms, are made, they are not yet deployable. [5]

2.2 Smart Cars as Challenges for Data Protection

The second presentation dealt with the challenges that smart cars pose for data protection. Smart or connected vehicles introduce technologies that were previously foremost associated with smartphones and big data analysis into the realm of road traffic ([6], pp. 201 et seq.). Motor vehicles have always been considered to be symbols of freedom and independence and as such they hold special meaning for society as a whole. In the Seventies, Germany's largest automobile club ADAC created the slogan "Freie Fahrt für freie Bürger" which loosely translates to "Free driving for free citizens" as a reaction to an initiative to limit the maximum speed on German motorways. The slogan has been exploited for numerous agendas since then, but its ongoing popularity still highlights that many people associate driving with freedom.
Cars in particular are seen as private spaces and despite the many windows and the need for adherence to traffic regulations, for social interaction and for cooperation with other drivers, most drivers seem to have high expectations of privacy when travelling in their cars.[1] The technical capabilities of smart cars allow for the collection of massive amounts of highly detailed personal data regarding the interior of the car, its surroundings, the communication between the driver and the car, the communication between the car and other motorists, the communication between the car and traffic infrastructure and infotainment. Such data can be compiled to create profiles regarding driving, usage, communication, movement, behaviour and relationships. These profiles can in turn be used to predict future actions. Thus, smart cars may not fulfil the promise of privacy and freedom that cars are usually associated with.

[1] For a detailed explanation of the concept of a car as a "private-in-public place" see [7].

Cars and driving affect and are affected by a number of basic rights; foremost those that guarantee mobility like Art. 45 I of the Charter of Fundamental Rights of the European Union (CFR, 2012/C 326/02), those that are concerned with life and integrity of the person like Art. 2 I and 3 I CFR, and those concerned with property like Art. 17 I CFR ([8], pp. 353 et seq.). However, mobility and safety are also prerequisites, means and requirements for instance for the freedom to choose an occupation and the right to engage in work (Art. 15 CFR), as well as the freedom to conduct a business (Art. 16 CFR). Furthermore, cars can be subject of research and thus Art. 13 CFR. Interconnectedness means that even more basic rights come into play; particularly the right to respect for private life and communications (Art. 7 CFR) and the right to protection of personal data (Art. 8 CFR) ([8], p. 354). We have to ensure that smart cars are designed in a way that aids in the exercise of these rights and does not hinder it ([9], pp. 391 et seq.).

The function of the law in general and of data protection law in particular in relation to smart cars is to secure freedom, responsibility and trust ([8], p. 357). The risks of use and abuse are determined by the intensity of the collected data, the value of the data and the manner and duration of data storage. Not too long ago, the extent to which cars were connected did not exceed the use of clunky car phones. The data collected by a smart car equipped with cameras, microphones and all kinds of sensors however will tell a lot about the status of the car, the behaviour of the driver, and much more. It is thus not difficult to imagine that numerous people and entities are affected by and may want to have access to that data: drivers, passengers, owners, renters, vehicle fleet management, manufacturers, suppliers, insurances, repair shops, towing services, emergency services, service providers, police, secret services, people involved in accidents, courts, government agencies, advertisers, market research companies and more (cf. [8], pp. 355 et sqq.; [10], p. 247). Some of the aforementioned may even be able to force access to the data. There can be a multitude of reasons for wanting the data: diagnosis, maintenance, evidence, insurance claims, to collect toll, infotainment, pay as you drive insurance models, geolocation, development of future car models, product liabilities, contractual liabilities and so on.

The data collected by the sensors of a connected car is personal data, if the data relates to an identified or identifiable natural person.[2] At least the owner of the car will usually be identifiable. The classification as personal data remains intact, even if the reference is false, for instance because another person is actually driving. The purpose of the collection will not always be clear or change at a later point in time, especially in the context of autonomous driving.

So who should be allowed to have access to data collected by a connected vehicle and under which conditions? Many manufacturers have a very clear opinion: The data is ours to use as we please. This is consistent with efforts to deprive car owners of the ability to perform maintenance and repairs. Future car owners may have a lot less control and authority over their cars than car owners today; going so far as to having

[2] For more details see [11], pp. 373 et seq.

to face their own cars as witnesses in a court case against them – figuratively speaking.[3]

The drivers become more and more transparent, while it becomes less transparent who has control over data, what the possibilities for control are, what data is actually collected and what is done with that data. This is intensified by the fact that in many countries telecommunications data retention laws are in place which means that any communication data to and from a connected car via internet or mobile telephony will be retained as well.

In the context of connected cars data collection, processing and storage are generally based on the data subject's consent. One notable exception and an example of data processing based on a legal obligation is the emergency call or short eCall system which will become mandatory for all new cars sold from April 2018 onwards.[4] The eCall system is a dormant system meaning that data is shared only in the event of an accident. The system then sends a predefined data set to a public safety answering point (PSAP) and automatically enables voice communication with the emergency telephone number 112.[5] This means that, among other things like a positioning system, a hands-free speakerphone has to be integrated into every car.

When it comes to consent, drivers are confronted with non-negotiable terms and conditions by the manufacturers. Furthermore, third party applications will usually be offered which will come with their own sets of terms and conditions. All of these have to be brought to the attention of the relevant persons. However, it cannot be expected that these persons will actually go through these documents as is the case with many other applications. Due to the fact that users are frequently confronted with lengthy terms and conditions, mostly via the screens of desktop computers or mobile devices, and that most users never experience any consequences as a result of accepting, many get used to simply accepting them without giving the matter much thought or even any thought at all. This is further complicated by the fact that software and hardware updates may add new capabilities, newly requiring consent. Consent becomes formalism instead of being an expression of private autonomy and self-determination with regard to the collection of personal data. On top of this, the requirement for consent is that it must be informed consent, when in reality data subjects do not know which data is ultimately collected and processed by whom ([11], pp. 376 et seq.).

A review of connected car privacy policies and terms of service, conducted by the British Columbia Freedom of Information and Privacy Association, indicates that many are in violation of data protection laws. The report states that there is a "lack of consent and forced agreement to unnecessary and arguably inappropriate uses such as marketing" and that standards such as "openness, accountability, individual access

---

[3] This could be a violation of 'nemo tenetur se ipsum accusare' ([12], p. 85).

[4] Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC.

[5] The eCall system is furthermore open to the implementation of additional telematics services, which also raises concerns regarding data protection and data security [13].

and limiting collection, retention, use and disclosure of customer data" are not met ([14], p. 6).

In November 2014, members of the Alliance of Automobile Manufacturers and the Association of Global Automakers[6] signed a commitment containing "Consumer Privacy Protection Principles" [15]. However, the principles set forth in the commitment offer a lower standard of data protection than what is already in place in the European Union and thus cannot serve as guidelines for the discussion in Europe.[7]

Another issue in the context of connected driving lies in the fact that it may not be possible for the data controller to identify whose data he processes. The owner of a car may have given consent, but what about passengers and other people driving the vehicle? Do they all have to be registered and give consent? The data of the holder of a pay-as-you-drive insurance policy may be processed based on the contract between him or her and the insurance. If a different person drives the car, that data may not be processed on the basis of the insurance contract, since he or she is not a contracting party. So that person would have to somehow give consent, since the processing of his or her data is an infringement of a fundamental right. And what about the following example: The 2016 Chevrolet Malibu will offer a "Teen Driver System" that will provide parents with a "report card" containing statistics such as maximum speed and distance driven [17]. This example illustrates the potential to control others that comes with all the sensors built into connected cars.

Yet another important issue is the use of dashboard cameras. While generally considered illegal in Germany,[8] some insurances in the UK even offer significant savings for users of dashboard cameras.[9] The possible scenario that within a Union that values free movement, an insurance company based in one country mandates the use of a certain device that is illegal in another, obviously poses problems. Another example for how cameras may be used in connected cars is a built-in video telephony system. This entails that a camera is aimed at the driver at all times.

Traffic infrastructure is also digitized. Examples for this are road toll systems, which use cameras to capture license plates and then check via a centralized database whether or not the vehicle registered under a captured license plate has paid the toll. Similar systems are used by police during manhunts and as an investigative measure, but also by private entities, for instance at parking lots to determine the parking duration. This means that cars that are not connected, not smart, may also leave a data trail.

In summary, the emergence of smart and connected vehicles raises the following questions: How can we enable drivers to make informed decisions regarding any data collected by a smart vehicle? How can we ensure transparency? Is the current concept of consent up to the task? In addition to these pressing challenges, there is the issue of cyber security.[10] Weaknesses in the sophisticated systems integrated into smart vehi-

---

6 Both are U.S. trade groups.

7 Nevertheless pleading for a vertical solution: [16].

8 Operating a dashcam is a violation of § 6b and 28 of the German Federal Data Protection Act ([18], pp. 363 et seq.). See also VG Ansbach, ruling of 12 August 2014, reference number AN 4 K 13.01634.

9 For example UK insurance company Swiftcover [19].

10 For an overview see [20].

cles could potentially be used to deliberately cause accidents.[11] Thieves and stalkers could also prey on such weaknesses. All in all, data security in connected cars is not just a matter of privacy, but a lack of security can also result in loss of property, serious bodily harm and even death.

Moreover, calls for back doors for electronic communication systems have been heard all over Europe and the U.S. in recent times.[12] Do we want to allow police officers to remotely access such systems, for instance to extract data in order to reconstruct where the driver went at what time, to create movement profiles? To allow them to use the microphones used by the eCall system for audio surveillance? Or maybe even to disable a car during a chase by activating the brakes? Already, U.S. auto lenders use GPS to track the movement of "subprime" borrowers and outfit cars with devices to remotely disable the ignition in case of non-payment (so-called "starter interrupt devices") [22].

The future of connected driving, an industry of particular importance to many European nations, hinges on finding solutions to these pressing challenges.

2.3 An Ethical Perspective on the Power of Smart Devices

In this part of the session, the idea was to highlight ethical issues of smart devices in order to foster a discussion on (potential) consequences and challenges and to provoke critical thinking. Therefore, a general overview was provided in the presentation which was structured along the questions: "Why should we talk about the ethics of smart devices?" and "What characteristics of smart devices might be ethically relevant and how may a conception of power help us to organise and inspire the discussion?" Three exemplary illustrations for an ethical reflection were provided subsequently.

Why Should We Talk about the Ethics of Smart Devices?

Ethics as a discipline is concerned with preconditions and evaluations of action. According to Hubig, ethical reasoning becomes necessary where 'there are specific characteristics of technology that shape the scope of possibilities to act' [23]. Ethical reasoning is important in order to avoid that technology determines the development of a society. A more application-oriented ethical approach (that is, however, not going to be pursued in the remainder of this contribution) would have to ask questions on how technology might or might not be used to benefit mankind or to prevent harm to entities that are endowed with a moral status.

Before highlighting and discussing some examples of (prospective) smart devices with regard to ethics, I want to give a brief overview of some conceptualisations of power that help to recognise and analyse power relations affecting the possibilities of humans to act. For this purpose, relational power approaches and especially a co-

[11] On the significance of IT security in cars with particular regard to embedded security see [21].

[12] Perhaps most impactful has been a speech by UK Prime Minister David Cameron given on 12 January 2015.

constitutive understanding of power are useful. Co-constitutive forms of power can be defined as 'internal relations of structural positions […] that define what kinds of social beings actors are' as well as their 'social capacities and interests' [24]. Furthermore, there are forms of power that constitute 'all social subjects with various social powers through systems of knowledge and discursive practices of broad and general social scope' [24]. Constitutive power (re)produces social identities, practices and authorisations of meaning and action [25].

Technologies play a vital part in co-constitutive power relations as they are more than only a neutral instrument or intermediate of power relations between individuals or institutions: technology has an effect on social relations (see [26], [27]). Following this understanding, smart devices are in a relation with humans that has an impact on humans' scope for action, on identities and interests of humans and on (power) relations between humans/social institutions.

This perspective on the role of technology shall serve as the background against which we look at three different illustrations of smart devices. By searching for and questioning the (co-constitutive) power relations that are influenced by smart technology, we can by no means grasp all ethical issues of smart devices. But we may enhance and structure our ethical reflection by highlighting effects on the scope of human action.

Reflection on Some Exemplary Illustrations.

Smart and Connected Cars .

The first illustration uses smart and connected cars as an example. By the introduction of a system of smart and connected cars the character of cars and its meaning for society change. Whilst traditionally a symbol of individual liberty and of the widespread mobility, the ability to go independently wherever and whenever, smart and connected cars are much more defined by being only a small part of a greater network. It is the network and its social and economic significance that becomes the most important aspect; and cars as the network's small cogs enable its functioning. Thereby, the values of the infrastructure, of the vendors and the environment are being inscribed into cars and represented by smart functions of cars. Concepts such as "efficiency", "security" or "environmentalism" gain power and govern the field, subsequently also influencing and judging the behaviour of car drivers in their way. It may even become a problem if people resist using smart cars as their behaviour then can be interpreted as asocial resistance against these values at the core of the system. To name only one consequence: those that do not want to take part in a smart car system, but stick to old technology could be charged higher insurance fees [28]. Based on these deliberations, we can assume that the perspective on car traffic changes completely. The traffic system providers, vendors and producers gain power over individuals by and rendering certain behaviours as appropriate and inappropriate.

Fitness Wearables.

The second illustration looks at fitness wearables such as smart watches, sleep and lifestyle trackers. Perhaps the most important aspect of fitness wearables is their con-

stant measuring and thereby also evaluating of the self. With these devices there comes an idea of normality that is inscribed in the practices of comparison of the data the device collects with certain pre-given "normal" behaviours and levels.

The comparison to a certain normality inscribed and always shown by the wearable changes the self-perception of individuals and also their relation and behaviour towards society. On the one hand, if the normal and the evaluation of the self diverges, there is the feeling of being abnormal or even ill. On the other hand, the envisaged effects are self-optimisation towards a goal that is written into and represented by the device. The device does not force people to obey and follow certain ways of life, but by its ubiquitous comparison to a normatively desired 'standard' and persuasive designs it enacts forms of self-governance. 'Even if a system were designed to only make suggestions, it would still find itself treading a fine line between inspiration and frustration, between obliging helpfulness and pig-headed patronization' [29].

The illustration of fitness wearables shows that data and smart devices can have power over individuals. But only if the devices are used and accepted, which is where we can observe the co-constitutive character. They do not unfold power by their own.

At the same time one can conceive of this kind of smart devices as having an empowering effect on humans by rising self-awareness. However, this self-awareness is based and influenced by the assessment of the self which has been conducted by others.

Virtual Reality and Decision Making.

The last illustration draws on an even more general characteristic of smart devices. By the usage of sensors measuring the environment, then calculating and processing the gathered raw data, interpreting it and eventually by visualising and evaluating the data, smart devices occupy a position between "reality" and individuals. Technology in these cases performs a mediating role and shows an enriched reality as many things that sensors can detect of our environments are not detectable in this way by humans. Furthermore, this reality is constantly being interpreted and evaluated.

As a consequence, smart devices can lead to better informed decisions as humans receive more information through technology than they could collect and process on their own. On the other hand, these decisions are of course highly influenced and biased by the working of the devices and the interpretations and processes that the engineers and developing companies have (unconsciously) built into their products. One has without a doubt to consider that there is not "one reality out there" that humans can eventually and objectively conceive. But in this case, we have to deal with a mediated "virtual" reality where mostly a company is the middleman. Furthermore, by using information from smart devices as a basis to our every-day decisions, these decisions become increasingly dependent on the (correct) working of smart devices. This leads to another question: if we base our decision deliberately and unconsciously on a virtual reality enhanced by smart devices, who is in the end responsible and to be held accountable for these decisions? Is it always the human, or also the smart device, respectively its producers? Can the technology be held responsible only if the information provided is "wrong" – and what is a wrong information? Or is it the relation

itself – the socio-technological system – that is responsible? And what are the consequences thereof in practice?

The issue of accountability becomes even more significant when we look at decision-making by technology itself, e.g. when algorithms of smart technologies assess the risk of air passengers. How can one assure that smart devices do not reproduce or reinforce discrimination or social sorting (see [30], [31])? And again, who is to be held responsible for these decisions that are taken by technology (see [32], [33])?

2.4 Regulating a Hyper-connected World

In this part of the workshop, the idea was to conclude the workshop with a general overview of recent regulatory challenges that derive from a hyper-connected world, which is most prominently referred to as the Internet of Things phenomenon. Starting with a brief terminology and description of the privacy challenges posed by the IoT, the following section is going to introduce into the different traditions in data protection regulation on either side of the Atlantic and into the most recent political debates in the US and EU on the regulation of the Internet of Things.

The Internet of Things as the backbone of a Hyper-connected World.

Early debates on the emergence of networked devices and information systems, which is nowadays most commonly referred to as the *Internet of Things*[13] or *IoT* date back to the early 1990ies. Back then, the gradually miniaturization of computers led to debates on *ubiquitous computing*, *pervasive computing* etc. [37], [38], [39]. During the 2000s, with the *Radio Frequency Identification* (RFID), it became possible to address specific devices within a short distance sensor network and to let them communicate with other RFID-capable devices [40]. However, all these technologies did not yet incorporate the internet into the devices. Instead, the notion of ubiquitous computing imagined relatively autonomous devices and the notion of RFID imagined primarily local networks. Only with the advent of communication protocols such as *IEEE 802.15.4*, *6LoWPAN* or *CoAP* and by outsourcing processing power into the cloud, the phenomenon which is today referred to as the internet of things, was finally brought to life.

Based on the promises of an increasingly connected world, a substantial change is predicted in at least five different markets. Firstly in the consumer market through fitness trackers, ambient assisted living systems and home automation, secondly, in the production chain and logistics sector through the industrial internet, thirdly, in the infrastructure sector through smart grids respectively smart meters, fourthly, in the healthcare sector through the data provided by e.g. fitness trackers or networked insulin devices and fifthly, in the agriculture industry ([41], 20 f.).

[13] The term *Internet of Things* was coined by a presentation by Kevin Ashton in 1999 ([34]). Highlighting the pervasive character of this development, the term *Internet of Everything* (IoE) ([35]) is also quite popular, while Weber ([36]) refers to it as the *Data of Things* respectively DoT.

Especially the commercial sector sees a big opportunity for innovation and further economic growth in the spread of connected technologies [42] and the extended usage of the collected data by new data literacy behaviours and big data analyses. Although personal data is not relevant in every one of the mentioned markets, for a lot of devices, applications and services, the collection and use of personal data is crucial. Unlike previous data collecting technologies, through the IoT not only more data, but also new kinds of data of any person within sensor range will be collected [43]. By transferring the data into the cloud and by performing big data analyses it is becoming increasingly unlikely, that an individual can keep in control which and how much of its data is collected by whom and processed or passed on to which instances for what purpose [36].

These privacy challenges lead to questions on how to deal with the future development of the IoT and how to engage these challenges by regulatory measures. However, during the past decades, two quite different traditions in the governance of data protection and privacy emerged across both sides of the Atlantic which also shape the current debates on the regulation of the IoT.

Regulatory traditions of data protection in the US and EU.

The EU approach to data protection regulation, which is often referred to as a comprehensive regime, relies - most prominently represented by the Data Protection Directive 95/46/EC - on a set of formal rules, which are derived from Fair Information Practice Principles and enforced across the public and private sectors through independent regulatory agencies. The US approach however, is considered as a limited regime by only applying formal rules on the public sector while relying mainly on sectoral privacy laws, self-regulation and technology in the private sector and at the same time in large parts lacking an institutional monitoring and enforcement of the legal framework [44]. These regimes, however, need to be considered as the formal side of the governance of privacy. Besides, due to the enormous speed of technological change, a major part of the regulation of privacy takes place at several global, regional and national levels of governance and involves a complex web of state-regulation, self-regulation and technology [45].

Regulatory fora and focus on either side of the Atlantic.

To date, there are no laws or an overarching national strategy by the US Congress, dealing specifically with the Internet of Things. Instead, at least two dozen separate federal agencies – ranging from the Federal Aviation Administration (FAA) to the National Highway Traffic Safety Administration (NHTSA) Food and Drug Administration (FDA) or the Department of Agriculture – and more than 30 different congressional committees deal with specific aspects of the IoT by usually realising mere statements. However, in the meantime, the FTC, which is responsible for privacy issues, emerged as the government's regulatory body for the IoT. Besides, the NHTSA and FAA are both grappling with IoT related issues such as driverless cars and drones, respectively [46]. The hearings, round tables and working groups, conducted by these administrations and committees usually follow a multi-stakeholder

path and involve representatives from technology industry, privacy groups and Congressional offices [47]. Although there is no concerted regulation strategy, the US' position on the regulation of the IoT can be described as a rather passive laissez-faire approach that is extremely cautious not to stiffle innovative business models that may emerge with the advent of the IoT. In this context, it is regularly pointed to the major influence of industry on even the most precocious steps in the field of IoT regulation in order to explain the cautious attitude of Congress [48].

Both, in the US and EU, a core component of the efforts in dealing with the IoT relates to device and network security, respectively data security and breach notification. In the US, data security legislation is the lowest common denominator in regulatory matters on which many of the relevant stakeholders can give their assent [49] and also the one demand on which the FTC have shown itself to be intransigent [50]. Different government policies regarding data security and cybersecurity show the increased attention this topic has received in the past on a federal scale. However, regarding data minimization, purpose limitation and notice and consent, the picture differs considerably. While the FTC recommends data minimization as one necessary step in order to achieve better data security and data protection, it still gives companies a lot of flexibility by proposing that they can decide not to collect data at all, collect only the fields of data necessary to the product or service being offered, collect data that is less sensitive or de-identify the data they collected. In the event that a company decides that none of these options work, the FTC recommends the company to seek consumers' consent for collecting additional, unexpected data [50]. The FTC's recommendations led to a series of harsh criticism from industry and other governmental bodies [51], [52]. Regarding notice and consent in the light of the emerging IoT sector, the FTC points that notice and choice are particularly important when sensitive (e.g. health) data is collected and that informed choice remains practicable, although it is not considered important in every data collection. In contrast, both other governmental as well as industry representatives share the opinion that potential new uses of data, leading to societal and economic benefits could be restricted by such measures and that a risk-based approach in dealing with the IoT should be favoured [53], [54], [46], [47], [48].

Contrary to the US approach, especially the EU Commission plays an active part in the regulation of the IoT. Based on the notion that the EU largely overslept the spread and development of the internet during the 1990ies and thus failed to compete with the US technology branch, the key idea behind the present activity of the EU is to not repeat the mistakes previously made and instead, to actively shape the emerging IoT markets. In this respect, the EU commission's work involves the establishment of several multi-stakeholder discussion groups and consultations involving representatives from industry and privacy groups that started around 2005 and initially focused on RFID and which finally led to the commission's action plan, that was presented back in 2009 [55], [56], [57]. In contrast to the US, the EU has a rather comprehensive IoT strategy that is centred around the activities of the European Commission that followed the 2009 IoT action plan.

At the moment, the EU General Data Protection Regulation and the creation of the Digital Single Market are considered to play a major role in shaping the regulatory

cornerstones of the future IoT regulation and a review of the ePrivacy Directive is scheduled for 2016 [58]. Within these efforts, the EU not only commits itself to data security, but – regarding data protection and privacy – also ”to the highest standards of protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights” ([58]; see also: [59]). Thus, similar to the Article 29 Working Party's opinion, data minimization, purpose limitation and notice and consent are still favoured in the sense of the Data Protection Directive [60]. However, in March 2015, when the Council's position on the debated Data Protection Regulation became known for the first time a possible policy shift was announced: In the light of the importance that is ascribed to data collections through the IoT and in order to be able to support big data markets with the amounts and quality of data required, especially nation states, organised within the EU council, were accused of attempting to change the formerly comprehensive EU data protection regime towards a more flexible one. Some privacy advocates feared that this could weaken the principles of purpose limitation and notice and consent [61] although such worries are deemed groundless by others [62]. On the bottom line, however, in all of the EU's activities a much greater focus on individual rights, data protection and the assessment of ethical problems is prevalent.

Especially in the context of a technology that is regarded as disruptive as the IoT sector currently is considered to be, proponents of the new technology usually urge governments not to stifle innovation and economic growth by hard legislation. Privacy advocates, on the other hand, warn of the significant privacy risks of a hyper-connected world and call for legislative reform. Furthermore, different traditions in the governance of privacy shape current governmental action in IoT regulation. Particularly the principles of data minimization, purpose limitation and notice and consent are subject of an ongoing debate on the regulation of the IoT. While the US favours a laissez-faire approach, the European Union has committed itself to establish more durable, technology neutral rules by the adoption of the General Data Protection Regulation by the end of the year. However, IoT regulation will most likely remain a current topic, as the evolution of the IoT will probably raise new privacy challenges.

3 Discussion and Concluding Thoughts.

The broad (technical) overview of major challenges concerning smart cars in the beginning raised several questions in the audience, especially remarks on own – personal and research – experiences with smart cars. The (potential) accessibility of the data for official authorities – mainly the police – was seen as very critical. In fact, in the past police authorities have used traffic information collected and shared by customers of a large navigation device and service provider to place speeding cameras. The short discussion after the “technical introduction” allowed a smooth transition to the legal part of the workshop, a presentation discussing Smart Cars as Challenges for Data Protection.

In the final discussion, we also had a more thorough look for instance at smart devices that are used in health systems. It was put forward that although there is a lot information and data gathered about the patient, it is above all the health company that

produces and runs the smart device/system and that is empowered by the vast amount of data gathered. A similar question was raised when discussing who is really empowered by disruptive apps and technologies that are used to run UBER cars.

In another part of the discussion we discussed that privacy is primarily defined as an individual value and as such, in argumentations it becomes subordinate to social values such as traffic security, efficiency or environmentalism. We reasoned therefore on the need to understand privacy as a social and collective value in order to compete and remain valid in conflicts of values that especially might evolve around smart technologies.

We may summarise here, that smart devices become an important part in existing and emerging power relations which can lead to value conflicts such as efficiency vs. privacy. Power relations can evolve in several ways: Humans may be empowered by intelligent devices; they may also be in a more dependent power-relation and thereby governed by the concepts, functions and decisions of smart devices; and furthermore, humans may self-govern themselves along smart devices' concepts and functions.

4 References

1. Hansen, M.: Das Netz im Auto & das Auto im Netz. Datenschutz und Datensicherheit 6/2015, p. 367-371 (2015)
2. Hansen, M.: Zukunft von Datenschutz und Privatsphäre in einer mobilen Welt. Datenschutz und Datensicherheit 7/2015, p. 435-439 (2015).
3. U.S. Government Accountability Office: In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers. GAO-14-81 (2013)
4. Kelly, T.: Consumers are in the Connected Car's Driver Seat in 2015. Wired, 28.01.2015 http://www.wired.com/2015/01/consumers-are-in-the-connected-cars-driver-seat-in-2015/ (last accessed: 24 November 2015)
5. Troncoso, C. et al.: On the Difficulty of Achieving Anonymity for Vehicle-2-X Communication. Computer Networks 55(14), 2011, 3199-3210 (2011)
6. Weichert, T.: Datenschutz im Auto – Teil 1. Straßenverkehrsrecht, 201-207 (2014)
7. Urry, J.: Inhabiting the car. The Sociological Review 54, Issue Supplement s1, 17-31 (2006)
8. Roßnagel, A.: Grundrechtsausgleich beim vernetzten Automobil. Datenschutz und Datensicherheit 6/2015, 353-358 (2015)
9. Rieß, J., Greß, S.: Privacy by Design für Automobile auf der Datenautobahn. Datenschutz und Datensicherheit 6/2015, 391-396 (2015)
10. Lüdemann, V.: Connected Cars. Zeitschrift für Datenschutz 6/2015, 247-254 (2015)
11. Buchner, B.: Datenschutz im vernetzten Automobil. Datenschutz und Datensicherheit 6/2015, 372-377 (2015)
12. Mielchen, D.: Verrat durch den eigenen PKW – wie kann man sich schützen? Straßenverkehrsrecht, 81-87 (2014)
13. Lüdemann, V.: Sengstacken, C.: Lebensretter eCall: Türöffner für neue Telematik-Dienstleistungen. Recht der Datenverarbeitung, 177-182 (2014)
14. British Columbia Freedom of Information and Privacy Association: The Connected Car: Who is in the driver's seat? FIPA, Vancouver (2015)

15. Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc.: Consumer Privacy Protection Principles, Privacy Principles for Vehicle Technologies and Services. Washington, D.C. (2014)
16. Sörup, T., Marquardt, S.: Datenschutz bei Connected Cars. Zeitschrift für Datenschutz 7/2015, 310-314 (2015)
17. Chevrolet, http://www.chevrolet.com/2016-malibu/ (last accessed: 23 November 2015)
18. Hornung, G.: Verfügungsrechte an fahrzeugbezogenen Daten. Datenschutz und Datensicherheit 6/2015, 359-366 (2015)
19. Swiftcover, http://www.swiftcover.com/carinsurance/dashcams/ (last accessed: 23 November 2015)
20. Krauß, C., Waidner, M.: IT-Sicherheit und Datenschutz im vernetzten Fahrzeug. Datenschutz und Datensicherheit 6/2015, 383-387 (2015)
21. Lemke, K., Paar, C., Wolf, M. (eds.): Embedded Security in Cars. Springer, Heidelberg (2006)
22. Corkery, M., Silver-Greenberg, J.: Miss a Payment? Good Luck Moving That Car. The New York Times, New York edition, 25 September 2014, A1
23. Hubig, C.: Die Kunst des Möglichen II. Ethik der Technik als provisorische Moral. Bielefeld, transcript (2007)
24. Barnett, M., Duvall, R.: Power in global governance. In: Barnett, M., Duvall, R. (eds) Power in Global Governance, pp. 1–32. Cambridge, Cambridge University Press (2005)
25. Foucault, M. Discipline and punish: the birth of the prison. London, Penguin Books (1991 [1977])
26. Latour, B.: Reassembling the Social. An Introduction to Actor-Network-Theory. Oxford, Oxford University Press (2005)
27. Acuto, M., Curtis, S. (eds.): Reassembling International Theory: Assemblage Thinking and International Relations. Basingstoke, Palgrave Macmillan (2014)
28. Morozov, E.: The rise of data and the death of politics. The Guardian (2014) http://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation (last accessed: 17 November 2015)
29. Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F., Rohs, M.: Living in a world of smart everyday objects – Social, economic, and ethical implications. Human and Ecological Risk Assessment 10(5), 763–785 (2004)
30. Gandy, O.H.: Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems. Ethics and Information Technology 12(1), 29–42 (2010)
31. Lyon, D. (ed.): Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. London/New York, Routledge (2003)
32. Himma, K.E.: Artificial agency, consciousness, and the criteria for moral agency: what properties must an artificial agent have to be a moral agent? Ethics and Information Technology 11, 19–29 (2009)
33. Johnson, D.G., Miller, K.W.: A dialogue on responsibility, moral agency, and IT systems Proceedings of the 2006 ACM symposium on Applied computing -- SAC '06. ACM Press, 272–276 (2006)
34. Ashton, K.: That 'Internet of Things' Thing. In: RFID Journal (2009) http://www.rfidjournal.com/articles/view?4986 (last accessed: 19 November 2015)

35. Bajarin, Tim: The Next Big Thing for Tech: The Internet of Everything. In: Time (2014) http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/ (last accessed: 19 November 2015)
36. Weber, Rolf H.: The digital future – A challenge for privacy?. In: Computer Law & Security Review. 31 (2), p. 234–242 (2015)
37. Weiser, Marc: The Computer for the 21st Century. Scientific American 265(9), p. 66-75 (1991)
38. Mattern, F.: State of the Art and Future Trends in Distributed Systems and Ubiquitous Computing. Vontobel TeKnoBase (2000)
39. Mattern, F.: Ubiquitous Computing. In: Kubicek, H.; Fuchs, G.; Roßnagel, Alexander (Hrsg.) *Internet @ Future, Jahrbuch Telekommunikation und Gesellschaft 2001*. S. 52–61 (2001)
40. Fleisch, E.; Mattern, F.: Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Berlin, Springer (2005)
41. Sprenger, F., Engemann, C.: Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt, Bielefeld, transcript Verlag, 7-58 (2015)
42. Gartner: Gartner says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022. In: Gartner Press Release, 08.09.2014 (2014) https://www.gartner.com/newsroom/id/2839717 (last accessed: 19 November 2015)
43. Swan, M.: Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. In: Journal of Sensor and Actuator Networks. 1 (3), 217–253 (2012)
44. Newman, A. L.: The Governance of Privacy. In: David Levi-Faur (ed.) The Oxford Handbook of Governance, pp. 599{611, Oxford University Press (2013).
45. Bennett, C. J., Raab, C. D.: The governance of privacy: policy instruments in global perspective. 2nd and updated ed. Cambridge Mass.: MIT Press, (2006).
46. Samuelsohn, D.: What Washington really knows about the Internet of Things. A Politico investigation. In: Politico, 2015/06 (2015) http://www.politico.com/agenda/story/2015/06/internet-of-things-caucus-legislation-regulation-000086 (last accessed: 19 November 2015)
47. Politico Staff: The Internet of Things: What's Washington's Role? A politico working group report. In: Politico, 2015/08 (2015) http://www.politico.com/agenda/story/2015/08/internet-of-things-mckinsey-working-group-000207 (last accessed: 19 November 2015)
48. Romm, T.: Round 1 goes to the lobbyists: A barely there technology is already winning the influence battle in Washington. Here's how. In: Politico, 2015/06 (2015) http://www.politico.com/agenda/story/2015/06/internet-of-things-government-lobbying-000097 (last accessed: 19 November 2015)
49. Peppet, S.R.: Regulating the internet of things: First steps toward managing discrimination, privacy, security & consent. In: Texas Law Review, forthcoming (2014).
50. Federal Trade Commission: Internet of Things. Privacy & Security in a Connected World. FTC Staff Report, January 2015 (2015)
51. Gross, G.: FTC calls on IoT vendors to protect privacy. PCWorld (2015) http://www.pcworld.com/article/2876332/ftc-calls-on-iot-vendors-to-protect-privacy.html (last accessed: 24. November 2015)

52. Diallo, A.: Do Smart Devices Need Regulation? FTC Examines Internet Of Things. Forbes (2013) http://www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/ (last accessed: 24. November 2015)
53. The White House: Big Data: Seizing opportunities, preserving values. May 2014 (2014)
54. President's Council of Advisors on Science and Technology: Report to the President. Big Data and Privacy: A technological perspective. May 2014 (2014)
55. European Commission: Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. 15.03.2007, Com(2007) 96 final (2007)
56. European Commission: Internet of Things – An action plan for Europe. Brussels, 18.06.2009, COM(2009) 278 final (2009a)
57. European Commission: Commission recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. Brussels, 12.05.2009, C(2009) 3200 final (2009b)
58. European Commission: A Digital Single Market Strategy for Europe. SWD(2015) 100 final (2015)
59. European Commission: Digital Agenda: Commission consults on rules for wirelessly connected devices - the "Internet of Things". Press Release, 12.04.2012, IP/12/360 (2012)
60. Article 29 Data Protection Working Party (2014): Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things. Adopted on 16 September 2014, 14/EN, WP 223.
61. Järvinen, H. (2015): Privacy and Data Protection under threat from EU Council agreement. 15.06.2015, Press Release by European Digital Rights and Privacy International. https://edri.org/press-release-privacy-and-data-protection-under-threat-from-eu-council-agreement/ (last accessed: 19 November 2015)
62. Richter, P.: Datenschutz zwecklos? - Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO. Datenschutz und Datensicherheit 11/2015, p. 735-740 (2015)