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

Andreas Baur-Ahrens, Felix Bieker, Michael Friedewald, Christian Geminn, Marit Hansen, Murat Karaboga, Hannah Obersteller

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 Institute for Systems and Innovation Research ISI, Karlsruhe, Germany
{michael.friedewald|murat.karaboga}@isi.fraunhofer.de
[4] Research Center for Information System Design, Kassel University, Germany
c.geminn@uni-kassel.de

Abstract. In this workshop we addressed what it means to live in a smart world with particular regard to privacy. Together with the audience, we discussed the impacts of smart devices on individuals and society. The workshop was therefore interdisciplinary by design and brought together different perspectives including technology, data protection and law, ethics and regulation. In four presentations, a range of issues, trends and challenges stemming from smart devices in general and smart cars in particular – as one example of an emerging and extensive smart technology – were raised. In the discussion, it became clear that privacy and its implementation are at the core of the relationship between users on the one side and smart appliances as well as the technical systems and companies behind them on the other and that there is an ongoing need to broaden the understanding of privacy in the direction of a social and collective value.

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

1 Introduction

Smart devices are invading 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 still acted as a window into the future by demonstrating the seemingly endless possibilities of a "smart world". Today, some smart devices and systems are already well established, for instance those that are concerned with assisted driving, whereas others, like smart glasses, remain experimental.

At this stage of the technological development of smart appliances, it is worthwhile

and necessary to have a thorough look at the effects and challenges that the technology poses to privacy. Coming from different professional and academic disciplines, we therefore provided four perspectives on smart devices in order to make an interdisciplinary contribution to their assessment.

(1) While some smart technologies, like smart cars, are comparatively new to the market and are still under development, the general challenges for privacy resulting from connection and interaction are not new at all. From a technical perspective, the question arises as to whether and how we can learn from experiences with internet and smart phone usage concerning data traces, profiling of users and a lack of transparency to foster a privacy-enhancing design of smart cars and their infrastructure.

(2) 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 constitutional rights like Germany's right to informational self-determination come into play.

(3) 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 hand over to technologies and technical systems? One way of addressing these questions is to look at the structural and diffuse power relations that govern the field. This is not only related to the power of smart technologies themselves, but also to the power of social actors enhanced by smart devices and the power of concepts, e.g. "efficiency" that might oppose values like individual privacy. A broad concept of power can help to evaluate the impact of a world of smart appliances.

(4) 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 and on a more generic level between socially desirable and unacceptable technological developments. With reference to the aforementioned legal and ethical perspectives, a political science point of view dealt with the question, which particular regulatory measures are taken into consideration in order to shape the digital future in a socially appropriate and sustainable manner.

Thus, the workshop was structured in a way that allowed for discussion and questions after the first half and at the end of the workshop. Therefore the first two presentations were focused on smart cars as one particular example of an emerging and potentially highly intrusive smart technology and examined them from both a technological and a legal perspective. The two following presentations also formed a unit. Here, we took a step back and emphasised on the ethical and regulatory issues of smart devices in general. In the concluding discussion, which was open to the floor, an interdisciplinary reflection took place.

2 Workshop Content

The workshop began with a short introduction by the organisers, giving a broad over-

view of the topic, including more general challenges and trends resulting from current technological developments in the field of smart devices. In the following, we summarise the input given in the presentations:

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

The workshop started with a presentation on the challenges for privacy arising from technology itself. It was aimed at giving the audience a basic understanding of the kind of data that is collected by a smart device, of data flows, as well as possibilities of tracking and profiling the user. In order to give a comprehensive example with great practical relevance, the presentation focussed on the privacy risks posed by smart cars, [1,2], which also allowed the elaboration of the economic exploitation of user profiles by private companies.

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 in the following talks. The starting point was a comparison of the rapidly advancing technologies behind smart cars with – already well-established – smart phones. It was argued that – from a technical point of view – the same data protection issues were present. Consequently, now that the number of smart cars is increasing and a strategy for handling upcoming issues has to be found, it is advisable to take a look back to earlier developments and learn from shortcomings, close gaps, and thereby create a framework which allows us to benefit from the technical progress, but which also respects the rights of individuals. Here, three main aspects have to be considered: Internet and telecommunications are used for functionalities provided in the car, information from and about the car is not only processed locally, but also in the external communication networks or even in data clouds, and finally, the car and its components have to be regarded as network nodes.

Smart cars, – every single component which makes the car a smart one – gather manifold kinds of data from manifold sources. Most of it is to be considered as personal data and as such falls under data protection legislation. The data is collected by several sensors, is transmitted with different techniques and is potentially stored and exploited in multiple ways. In smart cars, the following data concerning the vehicle is accumulated and accessible via the OBD-II-port ("On-Board Diagnostic System") in particular: the Unique Mobile Device Identifiers all mobile devices have, the numbers of SIM cards used for transfer of data needed for instance 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 for instance a smart phone with the car, RFID identifiers as they are needed for key remote controls. Whenever the respective devices or on board components communicate with the external world, this data is also transferred. Furthermore, information on the device setting (e.g. language) is communicated. This "phenomenon" is not new, but very similar to the functioning of internet browsers.

In addition to these issues already known from former technological achievements,

smart cars are equipped with multiple sensors, which measure the status of mechanical car components. This means that, for example, data on tire pressure, the state of engine and gears, as well as brake performance is collected and error messages are stored. Also, in most modern cars GPS transmitters are installed. They make it possible to collect data on the exact position of a car, the direction it is going, and generally deliver more precise results than what can be achieved by tracking the vehicle via speed mobile radio cells and WiFi hotspots [3]. Besides car data, data directly related to the driver and/or passengers is collected: The driver has 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 must be indicated. The smart car is able to store different preferred settings (from side mirrors to infotainment) for different drivers. Biometric data may be used to identify the driver as authorised to drive the car. Finally, some systems monitor and analyse driver medical data (e.g. heartbeat or eye movement) in order, for example, to detect signs of fatigue.

All this data is collected and can be extracted from the smart car. Yet, another parallel to former technological developments is that many business models to use this data in a meaningful way already exist or are under development. Car insurance companies that offer insurance policies following the 'pay-as-you-drive' model are just one example. This means that all relevant data from the car is analysed by the insurance company and an individual insurance rate is calculated accordingly.

Another example is the "expansion" of big mobile phone or IT companies into the automobile sector (mainly with the goal of integrating their system software into the car and facilitating a connection to their mobile devices) [4]. Just like internet user data, driver data can be analysed to offer more personalised and more specific services – like personalised maps or navigation services – which are able to take into account personal habits of the driver. This means, for instance, that the driver can choose not to drive routes which pass casinos or ex-partners' homes. All this data needs to be transferred to the service providers. This creates "usage patterns" just as they are known from internet usage. Data footprints allow the identification and tracking of the driver. Furthermore, due to the enormous volume of data that is collected, and of course for practical reasons, smart car data is often stored in the cloud. This raises the question of how it can be guaranteed that data is only used for the purpose it was collected, 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 a different quality of personal data as it brings together personal data on habits and activities, internet usage and health (e.g. control of eye movement) and therefore – especially in combination with personal settings – can be used to create very precise profiles of drivers. This makes the question of secure storage and access to those profiles even more delicate. Of course, these issues are well known from established online services. With respect to the developing market of smart cars, a repetition of history should be avoided.

Research on data-minimising techniques and methods for use in smart cars is ongoing. But although interesting approaches, such as a frequent change of pseudonyms have been put forward, they are not yet "market-ready" [5].

2.2 Smart Cars as Challenges for Data Protection

The second presentation dealt with the challenges that smart cars pose to data protection law. As demonstrated above, smart or connected vehicles introduce technologies that were previously predominantly associated with smartphones and big data analysis into the traffic arena ([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 people's association of 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] As shown in the first presentation, the technical capabilities of smart cars allow for the collection of massive amounts of highly detailed personal data which 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 adhere to the expectation of privacy and freedom that cars are usually associated with.

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 the subject of research and thus of 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 them ([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 sensitivity 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 will be affected by and may want to have access to that data: drivers, passengers, owners,

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

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 seq.; [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 such 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 etc..

The data collected by the sensors of a connected car is personal data, if the data relates to an identified or identifiable natural person (for more details see [11], pp. 373ff.). 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 may 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 to face their own cars as witnesses in a court case against them – figuratively speaking.[2] 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 in all new cars sold from April 2018 onwards [59]. The eCall system is a dormant system meaning that data is shared only in the event of an accident. The system sends a predefined data set to a public safety answering point (PSAP) and automatically enables voice communication with the emergency telephone number 112.[3] This means that – among other things – devices like a positioning system and 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 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

---

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

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

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, requiring new 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, whereas in reality, data subjects do not know which data is ultimately collected and processed, or 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 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* (both are U.S. trade groups) 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 that is already in place in the European Union and cannot serve as guidelines for the discussion in Europe.[4]

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 are processed. 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 company. 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.

Traffic infrastructure is also digitised. Examples for this are road toll systems, which use cameras to capture license plates and then check via a centralised database whether or not the toll was paid for the vehicle registered under a captured license plate. Similar systems are used by police during manhunts and as an investigative measure, but are also used by private entities, for instance at parking lots – to determine 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

[4] Nevertheless pleading for a vertical solution see [16].

legal 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 (for an overview see [18]). Weaknesses in sophisticated systems integrated into smart vehicles could potentially be used to deliberately cause accidents.[5] 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 also of security breaches which may 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.[6] 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. car hire companies use GPS to track the movement of "subprime" borrowers and outfit cars with devices to remotely disable the ignition in cases of non-payment (so-called "starter interrupt devices") [20].

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

Following the two presentations on smart cars as a comprehensive example of the use of smart technologies, the second part of the workshop broadened scope in order to discuss the ethical and regulatory implications of smart devices in general. In the third presentation, the ethical issues of smart devices in general were highlighted in order to foster a discussion on (potential) consequences and challenges and to provoke critical thinking. Three exemplary illustrations for an ethical reflection were subsequently provided.

Why Should We Talk about Ethics of Smart Devices? Ethics as a discipline is concerned with the preconditions and the evaluation of action. According to Hubig, ethical reasoning becomes necessary where 'there are specific characteristics of technology that shape the scope of possibilities to act' [21]. Ethical reasoning is important in order to avoid that technology determines the development of a society.

Before highlighting and discussing some examples of (prospective) smart devices with regard to ethics, a brief overview of some conceptualisations of power is provided in order to help in recognising and analysing power relations that affect the possibilities of humans to act. For this purpose, relational power approaches and especially a constitutive understanding of power are useful. Constitutive forms of power can be

---

[5] On the significance of IT security in cars with particular regard to embedded security see [19].

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

defined as 'internal relations of structural positions […] that define what kinds of social beings actors are' as well as their 'social capacities and interests' [22]. 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' [22]. Constitutive power (re)produces social identities, practices and authorisations of meaning and action [23].

Technologies play a vital part in co-constitutive (i.e. mutually reproducing) 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 [24,25]). Following this understanding, smart devices are in a relationship with humans that has an impact on humans' scope for action, on identities and interests, and on (power) relations between individuals and between individuals and social institutions.

This perspective on the role of technology served as the background against which we looked 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. However, we may enhance and structure our ethical reflection by highlighting effects of smart technologies on the scope of human action.

Reflection on Some Exemplary Illustrations. *Smart and Connected Cars.* The first case study picks up the example used in the previous presentations. By the introduction of a system of smart and connected cars, the character of cars and their 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 are represented by the 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 can then be interpreted as antisocial resistance against the values at the core of the system. To name only one consequence: those who do not want to take part in a smart car system, but stick to old technology could be charged higher insurance fees [26]. Based on these deliberations, we can assume that the perspective on car traffic will change completely. The traffic system providers, vendors, and producers gain power over individuals by rendering certain behaviours appropriate or inappropriate.

Fitness Wearables. The second example looked at fitness wearables such as smart watches or sleep and lifestyle trackers. Perhaps the most important aspect of fitness wearables is their constant measuring and thereby the constant evaluation of the self. With these devices 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 average values.

The comparison to a certain normality inscribed and always shown by the wearable changes the self-perception of individuals and their relationship and behaviour towards society. On the one hand, if the normal and the evaluation of the self diverge, 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 design 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' [27].

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 on their own.

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

Virtual Reality and Decision Making. In the last illustration, we drew on an even more general characteristic of smart devices. By using 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 in 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. Then again, these decisions are of course highly influenced and biased by the functioning 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 a company is the middleman. Furthermore, by using information from smart devices as a basis for our everyday decisions, these decisions become increasingly dependent on the (correct) functioning of the smart devices. This leads to another question: if we base our decisions deliberately and unconsciously on a virtual reality enhanced by smart devices, who is ultimately responsible and to be held accountable for these decisions? Is it always the human being, or also the smart device, respectively its developers or retailers? Can the technology be held responsible only if the information provided is "wrong" – and what is 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 auton-

omous decision-making by technology, e.g. when algorithms of smart technologies assess the risk to aviation security posed by individual air passengers. How can one assure that smart devices do not reproduce or reinforce discrimination or social sorting (see [28,29])? And again, who is to be held responsible for these decisions that are taken by technology (see [30,31])?

We may summarise from an ethical perspective that smart devices are becoming an important part in existing and emerging power relations and that this 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 be governed by the concepts, functions and decisions of smart devices; and finally, humans may even self-govern themselves along the concepts and functions of smart devices.

2.4 Regulating a Hyper-connected World

For the final part of the workshop, we concluded with a general overview of the recent regulatory challenges that derive from a hyper-connected world. However, the discussion on the regulation of smart devices, which has been ongoing for some time now, is recently most prominently referred to under the heading 'Internet of Things' (IoT). Starting with a brief terminology and description of the privacy challenges posed by the IoT, the following section introduces the different traditions in data protection regulation on either side of the Atlantic and the most recent political debates in the US and the EU on the regulation of the IoT, as these two trading blocks are most likely to have a major impact on the emerging IoT market.

The Internet of Things as the Backbone of a Hyper-connected World. Early debates on the emergence of networked devices and information systems – which in their entirety are nowadays most commonly referred to as the *Internet of Things*[7] – date back to the early 1990's. Back then, the gradual miniaturisation of computers led to debates on *ubiquitous computing*, *pervasive computing* etc. [35]. During the 2000s, with *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 [36]. However, these technologies did not yet incorporate the internet. Instead, the notion of ubiquitous computing envisioned relatively autonomous devices, and the notion of RFID envisioned 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, did the phenomenon which is today referred to as the Internet of Things, finally come to life.

Based on the promises of an increasingly connected world, a substantial change is

[7] Whereas the term smart device describes the concrete technical artefact, the term *Internet of Things* was coined by a presentation by Kevin Ashton in 1999 in order to describe the broader phenomenon of interconnected smart devices [32]. Highlighting the pervasive character of this development, the term *Internet of Everything* (IoE) [33] is also quite popular, while Weber [34] refers to it as the *Data of Things* respectively DoT.

predicted in at least five different markets. First, in the consumer market through fitness trackers, ambient assisted living systems, home automation and mobility services such as Uber or iDrive by BMW; second, in the production chain and logistics sector through the industrial internet; third, in the infrastructure sector through smart traffic, smart grids and smart meters; fourth, in the healthcare sector through the data provided by e.g. fitness trackers or networked insulin devices, and finally, in the agriculture industry ([37], pp. 20 et seq.).

The commercial sector, in particular, sees a big opportunity for innovation and further economic growth in the spread of connected technologies [38] and the extended usage of collected data through new data literacy behaviours and big data analyses. Although personal data is not relevant in all of the aforementioned 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 is more data, but also new kinds of data of any person within sensor range collected, as described in sections 2.1 and 2.2 [39].

The privacy challenges emerging from this development [34] lead to questions as to how to deal with the future development of the IoT and how to engage these challenges with regulatory measures. However, during the past decades, two quite different traditions in the governance of data protection and privacy emerged on 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 European 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 and its successor, the Data Protection Regulation – on a set of formal rules, which are derived from fundamental rights and freedoms, 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 to 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 mechanism [40]. These regimes, however, need to be considered as the formal side of the governance of privacy. Besides these, due to the enormous speed of technological change, a major part of the regulation of privacy takes place at numerous global, regional and national levels of governance and involves a complex web of state-regulation, self-regulation and technology [41].

Regulatory Fora and Focus on Either Side of the Atlantic. To date, there are no laws or an overarching national strategy put forward by US Congress, dealing specifically with the IoT. Instead, at least two dozen separate federal agencies – ranging from the Federal Aviation Administration (FAA) to the National Highway Traffic Safety Administration (NHTSA), the Food and Drug Administration (FDA) and the Department of Agriculture – and more than 30 different congressional committees deal with specific aspects of the IoT, usually publishing nothing more than non-binding statements. In the meantime, the Federal Trade Commission (FTC), which is

the foremost authority on privacy issues, emerged as the government's regulatory body for the IoT, while the NHTSA and the FAA are both grappling with IoT related issues such as driverless cars and drones, respectively [42]. The hearings, round tables and working groups conducted by these authorities and committees usually follow a multi-stakeholder path and involve representatives from the technology industry, privacy groups and Congressional offices [43]. Although there is no concerted regulation strategy, the position of the US on the regulation of the IoT can be described as a rather passive "laissez-faire" approach that is extremely cautious not to stifle innovative business models that may emerge with the advent of the IoT. In this context, it is regularly pointed to the major influence of the industry on even the most minimal steps in the field of IoT regulation in order to explain the cautious attitude of Congress [44].

Both in the US and EU, a core component of efforts in dealing with the IoT relates to device and network security, most notably 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 [45] and also the one demand on which the FTC has shown itself to be intransigent [46]. Different government policies regarding data security and cybersecurity show the increased attention this topic has received in the past on a federal level. However, regarding data protection, including its principles of data minimisation, purpose limitation and the data subject's rights to information and consent, the picture differs considerably. While the FTC recommends data minimisation 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, to collect only the types of data necessary to the functioning of the product or the service being offered, to collect data that is less sensitive or to 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 [46]. The recommendations of the FTC led to a series of harsh criticism from industry and other governmental bodies [47,48]. Regarding informed consent in the light of the emerging IoT sector, the FTC points out 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 [42,43,44], [49,50].

Contrary to the US approach and besides the various national strategies of EU Member States, the European Commission plays an active part in the formal regulation of the IoT [51]. This is mainly based on the notion that European industry – but also politics in its task of supporting economic development – largely overslept the development of the Internet during the 1990s and the spread of smart devices since the middle of the last decade and thus failed to keep up with US and Asian competitors in the microelectronics sector such as with personal computers, home entertainment and smart mobile telephony. As a result, the key idea behind the present activi-

ties of the European Commission is to not repeat the mistakes previously made and instead, to actively shape emerging IoT markets. In this respect, the work of the European Commission involves the establishment of several multi-stakeholder discussion groups and consultations – involving representatives from industry and privacy groups – that started around 2005. Initially, they focused on RFID, which finally led to an action plan, that was presented back in 2009 [52,53,54] and which has, since then, shaped the rather comprehensive IoT strategy of the EU.

At the moment, the EU General Data Protection Regulation (GDPR) and the creation of the Digital Single Market are considered as playing a major role in shaping the regulatory cornerstones of the future IoT regulation. Furthermore, a review of the ePrivacy Directive is scheduled for 2016 [55]. Within these efforts and in contrast to the US approach, the EU not only commits itself to foster the free flow of information but also to enhance data security and – regarding data protection and privacy – also to adhere 'to the highest standards of protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights' ([55]; see also: [56]). Thus, in line with the opinion of the Article 29 Working Party, data minimisation, purpose limitation and the data subject's right to information and consent are still favoured in the sense of the Data Protection Directive [57]. Although the worst fears of privacy groups about the weakening of the principles of purpose limitation, information and consent by the Council of Ministers [58] appear rather unfounded in the face of the final text of the GDPR, only the future will tell, how these general principles will be applied, for example through Codes of Conduct, positions, guidance or decisions by DPAs, through court decisions or through an intervention by the European Data Protection Board (EDPB). In the bottom line, however, in all of the activities of the EU, is that there is a much greater focus on individual rights, data protection and the assessment of ethical problems in comparison to the US.

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, whereas privacy advocates warn of the significant privacy risks of a hyper-connected world and call for legislative reform. Furthermore, different traditions in the understanding and governance of privacy shape current governmental action in IoT regulation. Particularly the principles of data minimisation, purpose limitation and informed consent will remain both in the US and – despite the agreement on the GDPR – in the EU 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 which enable the free flow of information while still being able to provide a high level of protection of fundamental rights. 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 first

part of the workshop raised several questions from the audience, as well as remarks concerning their own – personal and research – experiences with smart cars. The (potential) accessibility of the data for official authorities – mainly the police – was viewed very critically. In fact, it was put forward that 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.

In the final discussion, we considered certain technologies more carefully, for instance smart devices that are used in health systems. It was stated that, although there is a lot of information and data gathered about the patient, it is, above all, the health company that produces and runs the smart device/system that is empowered by the vast amount of data gathered. A similar question was raised when discussing who is really empowered by the apps and technologies that are used to run Uber cars that have a disruptive effect.

We realised that privacy is primarily defined as an individual value and as such, it is often deemed 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 a democratic society in order to compete and remain valid in the conflicts of values that simmer around smart technologies.

In summary, the workshop showed that smart devices are becoming an increasingly important part in our lives. They pose severe challenges to current legal systems and they demand regulation and technology design that ensures that the technological capabilities and business possibilities of smart devices are not the only driving forces, but instead that fundamental legal and ethical values are taken into account. We should keep in mind that privacy is foremost a fundamental right and has to be upheld in the face of technological advancement. This stems from the acknowledgement that it is an important societal value which affects the relationship, not only between humans, but also between humans, the technologies they use and the systems, companies and institutions behind them. The goal of the workshop, which was to look at the manifold societal challenges from a multitude of disciplinary perspectives in a condensed way, and to bring together these perspectives, has been achieved.

Acknowledgement: 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”. For more information see: http://www.forum-privatheit.de

References

1. Hansen, M.: Das Netz im Auto & das Auto im Netz. Datenschutz und Datensicherheit 6/2015, 367-371 (2015)
2. Hansen, M.: Zukunft von Datenschutz und Privatsphäre in einer mobilen Welt. Datenschutz und Datensicherheit 7/2015, 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. Krauß, C., Waidner, M.: IT-Sicherheit und Datenschutz im vernetzten Fahrzeug. Datenschutz und Datensicherheit 6/2015, 383-387 (2015)
19. Lemke, K., Paar, C., Wolf, M. (eds.): Embedded Security in Cars. Springer, Heidelberg (2006)
20. Corkery, M., Silver-Greenberg, J.: Miss a Payment? Good Luck Moving That Car. The New York Times, New York edition, 25 September 2014, A1
21. Hubig, C.: Die Kunst des Möglichen II. Ethik der Technik als provisorische Moral. Bielefeld, transcript (2007)
22. 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)
23. Foucault, M. Discipline and punish: the birth of the prison. London, Penguin Books (1991 [1977])
24. Latour, B.: Reassembling the Social. An Introduction to Actor-Network-Theory. Oxford, Oxford University Press (2005)
25. Acuto, M., Curtis, S. (eds.): Reassembling International Theory: Assemblage Thinking and International Relations. Basingstoke, Palgrave Macmillan (2014)
26. 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)
27. 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 Ecologi-

cal Risk Assessment 10(5), 763–785 (2004)
28. 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)
29. Lyon, D. (ed.): Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. London/New York, Routledge (2003)
30. 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)
31. 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, pp. 272–276 (2006)
32. Ashton, K.: That 'Internet of Things' Thing. In: RFID Journal (2009) http://www.rfidjournal.com/articles/view?4986 (last accessed: 19 November 2015)
33. 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)
34. Weber, Rolf H.: The digital future – A challenge for privacy?. In: Computer Law & Security Review. 31 (2), 234–242 (2015)
35. Weiser, Marc: The Computer for the 21st Century. Scientific American 265(9), 66-75 (1991)
36. Fleisch, E.; Mattern, F.: Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Berlin, Springer (2005)
37. Sprenger, F., Engemann, C.: Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt, Bielefeld, transcript Verlag, pp. 7-58 (2015)
38. 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)
39. 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), pp. 217–253 (2012)
40. Newman, A. L.: The Governance of Privacy. In: David Levi-Faur (ed.) The Oxford Handbook of Governance, pp. 599-611, Oxford University Press (2013).
41. Bennett, C. J., Raab, C. D.: The governance of privacy: policy instruments in global perspective. 2nd and updated ed. Cambridge Mass.: MIT Press, (2006).
42. 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)
43. 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)
44. 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)
45. Peppet, S.R.: Regulating the internet of things: First steps toward managing discrimination, privacy, security & consent. In: Texas Law Review, forthcoming (2014).
46. Federal Trade Commission: Internet of Things. Privacy & Security in a Connected World. FTC Staff Report, January 2015 (2015)
47. 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)
48. 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)
49. The White House: Big Data: Seizing opportunities, preserving values. May 2014 (2014)
50. President's Council of Advisors on Science and Technology: Report to the President. Big Data and Privacy: A technological perspective. May 2014 (2014)
51. Gabriel, P., Gaßner, K., Lange, S.: Das Internet der Dinge – Basis für die IKT-Infrastruktur von morgen. Anwendungen, Akteure und politische Handlungsfelder. Institut für Innovation und Technik. Berlin: Feller (2010)
52. European Commission: Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. 15.03.2007, Com(2007) 96 final (2007)
53. European Commission: Internet of Things – An action plan for Europe. Brussels, 18.06.2009, COM(2009) 278 final (2009a)
54. 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)
55. European Commission: A Digital Single Market Strategy for Europe. SWD(2015) 100 final (2015)
56. 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)
57. 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.
58. 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)
59. 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. O.J. L 123, (19.5.2015)