From the Mind to the Cloud: Personal Data in the Age of the Internet of Things

Giuseppe Lugano, Martin Hudák, Matúš Ivančo, and Tomáš Loveček

Abstract Society is undergoing a major digital transformation affecting all areas of human activity. While the expected benefits of this societal turn are many, the use of IoT technologies presents challenges and risks from the viewpoint of fundamental human rights, such as privacy, that should not be underestimated. The legislative framework is constantly adapting to address these emerging needs: in Europe, the introduction of the General Data Protection Regulation (GDPR) was a milestone towards an enhanced citizens' data protection. However, the GDPR does have its limitations, both from the viewpoint of its practical applicability and the grey areas, mostly related to specific technologies and applications. Two case studies are presented, namely on connected and automated driving and domestic social robots. Despite the GDPR, mechanisms allowing citizens to have adequate control over their personal data are still not in place, and the advent of the IoT is likely to increase such challenges.

Keywords Data protection · GDPR · Internet of Things · Connected and automated driving · Domestic social robots · Human–robot interaction

1 Introduction

Advanced information societies are undergoing a deep and most likely irreversible digital transformation, affecting its technological, socioeconomic, spatial, and cultural foundations. The notion of digital transformation has been increasingly used in many specific contexts such as smart cities (Harmon, Castro-Leon, & Bhide, 2015; Salem, 2016), digital literacy (ICT Panel, 2002), organizational change (Bounfour, 2016; Seufert & Meier, 2016), or innovative provisions of public services such as

G. Lugano (✉) · M. Hudák
ERAdiate team, University of Žilina, Žilina, Slovakia
e-mail: giuseppe.lugano@uniza.sk; martin.hudak@erachair.uniza.sk

M. Ivančo · T. Loveček
Faculty of Security Engineering, University of Žilina, Žilina, Slovakia

Y. Zhou, M. H. Fischer (eds.), *AI Love You*,
https://doi.org/10.1007/978-3-030-19734-6_6

health care (Agarwal, Gao, DesRoches, & Jha, 2010; Herrmann et al., 2018). Typical goals of digital transformation—a complex socio-technical process that involves an interplay among people, technologies, and institutions—are higher productivity, cost efficiency, reliability, and accessibility. In this chapter, digital transformation is understood more broadly as the transformative effect of Information and Communication Technologies (ICTs) and their effect on human activities and people's social lives (Taipale, 2009; Wajcman, 2015). The use of transformative technologies is not only changing transport, mobility lifestyles, ways of learning, and working but also the meanings and practices of friendship, romances, and the whole notion of intimacy (Hobbs, Owen, & Gerber, 2017).

Since the turn of the millennium, the Internet and the smartphone have been at the center of digital transformation, given their daily use by billions of people worldwide. As Lugano (2010) pointed out, this transformative effect is particularly prominent when conceptualizing the smartphone as a general-purpose platform for attaining individual and/or collective purposive action goals. From this perspective, the smartphone has "an enabling role and an emancipatory function for digital communities because it provides, through community-generated services (CGS), an increased capability to drive change." It is recognized that always-on digital devices such as smartphones and tablets should be regarded as powerful double-edged technological weapons: to maximize benefits, while alleviating risks, they should be handled with care and wisdom. Hence, participation in the digital world requires awareness of today's reality and its ambiguities, risks, and opportunities. The Internet and smartphones, particularly when considered from the viewpoint of social media, are powerful dual-use technologies: depending on how they are used, they can be beneficial or harmful. Unlike traditional weapons, it is not the device itself (e.g., the smartphone) that is harmful, but rather the data that such device produces about us, either silently in the background (e.g., through its sensors) or more explicitly as part of our social communication and activity with apps.

From the perspective of an individual, two interrelated trends of digital transformation are illustrated within this chapter. The first trend concerns the increasing types of personal data, previously invisible, inaccessible, or just intimately kept in people's intimate spheres which are nowadays continuously logged, quantified, gamified, and presented explicitly not only back to the person but sometimes also shared with his or her own social circles—even made public. To maximize its preservation, alleviate risks of loss and enable portability, personal data—even of sensitive nature—will be less and less stored just in physical form (e.g., paper) and kept in a single device (smartphone memory) or digital support (e.g., DVD, USB stick, and computer hard drive). In short, personal data will be increasingly moving from people's minds and hearts to the cloud. The second trend is that despite technical enforcements, efforts to explain and simplify personal privacy managements to users, and legislative adaptations such as—in Europe—the European General Data Protection Regulation (GDPR)[1] it is still practically impossible to gain full

[1] EU Regulation (EU) 2016/679 of the European Parliament and of the Council—Article 94—Repeal of Directive 95/46/EC.

control of one's own data once this is collected and uploaded to the even-expanding Internet cloud. And the situation is not expected to improve in the near future with the next step of the digital transformation—the Internet of Things (IoT). The IoT will further integrate aspects of the physical and digital world, pushing further the blurring of the boundaries of the wider consequences of the process of digital convergence (Lugano, 2010). Moving from this consideration, Baldini, Botterman, Neisse, and Tallacchini (2018) call for an ethical design of the IoT based on a policy-based framework, which is "*respectful of the rights of the citizens instead of being only driven by economic considerations*." According to this view, new approaches to privacy and data protection are needed since "the amount of collected data from the IoT will be too difficult to control—and the complexity becomes even higher when attempting to determine which data are personal and which are not" (Baldini et al., 2018).

Interestingly, in the months before the introduction of the GDPR, the "Facebook—Cambridge Analytica" case occupied the global media headlines, with a strong impact on business and political discussions.[2] This was probably the largest personal data scandal in history, involving the use of personal data collected since 2014 from at least 87 million Facebook users, mostly from the USA, for a purpose (i.e., influencing political opinions) that was different than the declared one (i.e., carrying out academic research). The unprecedented opportunities that smartphones and social media offer to study human behavior correspond to new risks for influencing and manipulating opinions and behaviors at local, national, and global levels (Gross, 2018).

Many other stories could be reported on inappropriate uses of personal data. An interesting one was published by *The Guardian* in July 2017 on data collected by Tinder, a popular dating smartphone app. Judith Duportail, journalist and author of this story, found that that the company behind Tinder gathered a "dossier" of over 800 pages on the journalist, based on her Tinder use and about 1700 messages exchanged. The official purpose for dating apps to collect all such data is to "personalize the experience for each of our users around the world" (Duportail, 2017) by means of advanced algorithms that are part of the core company technology and therefore protected as intellectual property. In short, details on such algorithms and ways in which personal sensitive data is processed cannot be revealed to the user. Luke Stark, digital technology sociologist at Dartmouth University, provided his comment on the story, underlining that "Apps such as Tinder are taking advantage of a simple emotional phenomenon; we can't feel data. This is why seeing everything printed strikes you. We are physical creatures. We need materiality." This is one of the key aspects of the digital transformation, to which we, as human beings, cannot easily and rapidly adapt.

Nandwani and Kaushal (2017) carried out a study on the vulnerability of users to privacy disclosures in online dating applications such as Tinder. According to the authors of the study, in <30 min they could collect from most users personal data

[2] The Cambridge Analytica Files. *The Guardian*. Available at https://www.theguardian.com/news/series/cambridge-analytica-files.

such as full name, date of birth, phone number, personal photo, email address, and work occupation details. This is an example of social engineering attack (Krombholz, Hobel, Huber, & Weippl, 2015), which has become very popular in the age of always-on smartphone connectivity and social media.

In the IoT context, the collection of personal data and personal sensitive data will affect not only personal computers and smartphone apps but also a large amount of smart devices including connected and automated vehicles and domestic robots used for companionship or even for sex (Cheok, Levy, Karunanayaka, & Morisawa, 2017; Danaher & McArthur, 2017; Sharkey, van Wynsberghe, Robbins, & Hancock, 2017). In these contexts, data will be often collected through natural interactions and conversations with virtual assistants (Lugano, 2017).

Entering this digital world is easy and convenient and may be used for "flight" instead of "fight" whenever needed. However, this sense of freedom and power is an illusion: while access, creation, and the sharing of data (in any form) is rather easy, gaining full control over one's own personal data is practically impossible. Once shared, data can be copied and stored locally; it is not possible to know how many copies exist, who has access to them, and how they are used. The discussion on the "right to be forgotten" (Newman, 2015), with different views and interpretations across the world, represents only the tip of the iceberg of the whole issue of personal data control. Feelings of frustration and the need to regain control contribute to the rise of phenomena such as *digital paranoia* (McNeal & Schmeida, 2015) and *digital detox* (Miksch & Schulz, 2018; Ugur & Koc, 2015). These reactions may also lead to new forms of exclusion and digital divide, especially among weaker social groups (Baldini et al., 2018). Other worrying practices related to the misuse of sensitive data are sexting and revenge porn, which often involve teenagers (Englander, 2015), and increasingly happen among strangers who meet online. How do we protect users from these negative trends in the age of ubiquitous and pervasive computing?

Ensuring adequate control over personal data is one of the greatest challenges of being part of a digital world. Many parallel developments aim at addressing the challenge of control over personal data at various levels: at a technological level (e.g., facial recognition software to detect misuse of images), at an educational level (e.g., promoting digital civility), and at a legal level (e.g., introduction of the GDPR in the European Union). In line with the view presented by Baldini et al. (2018), we claim in this chapter that all the ongoing data protection developments are not yet adequate to address the challenges of the IoT. This claim is illustrated in the chapter as follows: after an overview on how the GDPR aims at further protecting users in the European Union, we make specific reference to the processing of personal sensitive data in the area of connected and automated driving (CAD) and domestic social robots with an advanced artificial intelligence (AI). The two areas have been selected due to being related to each other, and therefore useful to understand ongoing trends and future developments. In particular, CAD is the first major IoT area that will most likely affect lives of billions of people worldwide in the next few years. In CAD, being connected means that vehicles will be able to exchange information wirelessly with other vehicles and infrastructure as well as with the vehicle manufacturer and/or third-party service providers. Vehicle connectivity enables a communication that is cooperative, not competitive. Technically, this is described as cooperative intelligent transport systems (C-ITS), an area of ITS that focuses on vehicles' connectivity and cooperative communication. In addition to being connected, CAD vehicles will also be increasingly automated in some aspects of safety-critical control functions without direct driver input. While CAD will materialize in the next wave of intelligent cars and transport systems, domestic social robots and advanced AI will be less visible as they will be gradually embedded and penetrate all forms of digital technologies and devices, including CAD. Like smartphones, CAD will also collect large amounts of personal data, which will be aggregated and processed by advanced AI. Part of the processed data will also be used to enhance the user experience and provide further service options to the user through smart interfaces and virtual assistants (a form of social robot). This form of value creation, largely dependent on the collection and aggregation of user's personal data with other data sources, is challenged by the need to strengthen the protection of the same personal data. Although personal data collection is typically assessed by taking into account both the privacy and the (cyber-)security perspectives, in this chapter we primarily focus on personal privacy implications. The chapter concludes by pointing out areas in need of further investigation, underlining the importance of dialog and collaboration among the research community, policymakers, and business actors.

2 GDPR and Data Protection in the IoT

This section frames the discussion on personal data and the GDPR requirements in relation and context to the IoT. Specifically, while IoT technologies are designed for end users, the GDPR requirements and measures are largely addressed to companies responsible for the collection and processing of personal data. To what extent can users be empowered and gain control over their data? While a trade-off among value creation and user protection is understandable, users cannot easily influence such decisions, as their perception, awareness, and actual control over data are strongly influenced by companies' corporate communication and GDPR-compliant design of devices and user interfaces.

The Internet of Things has been defined as "an emerging global Internet-based information architecture facilitating the exchange of goods and services in global supply chain networks" (Weber, 2010). Regarded as an information architecture, privacy and security are typically described as IoT technology requirements related to the "concealment of personal information as well as the ability to control what happens with this information" (Weber, 2010). To the end user, the IoT may be more simply explained as a "collection of "things" embedded with electronics, software, sensors, actuators, and connected via the Internet to collect and exchange data with each other" (Yang, Wu, Yin, Li, & Zhao, 2017).

The IoT extends the Internet as it is known today by interconnecting objects of everyday use. A 2017 report on the IoT by Gartner estimated that 20 billion devices will be connected by 2020 (Hung, 2017). Compared to the "first wave" of digital transformation, symbolically associated to always-on connected smartphones, IoT is the next wave of digital transformation enabling many devices of everyday use, such as the car, fridge, or television, to be always-on and interconnected. This means that all the devices, similarly smartphones, will also be continuously collecting and processing personal data—sometimes of sensitive nature. Such data will be stored in company servers, typically based on cloud computing technology. As a valuable asset, criminals will be interested to find out creative and innovative ways to exploit vulnerabilities to realize their own interests. For this reason, privacy and security requirements for the IoT represent one of the key areas that will determine the success, or the failure, of the associated products and services strongly influenced by customers' trust.

In parallel to the enforcement of technological solutions put in place by businesses, public authorities contribute by updating the data protection legislative framework. In this respect, the introduction of the GDPR in Europe represents an important step for strengthening citizens' data protection rights in terms of increased transparency and awareness on how collected personal data is used. In the GDPR,[3] personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Specific identifying factors include in particular:

(a) *Genetic data*: personal data concerning inherited or acquired genetic characteristics of a natural person and providing unique information on the physiology or health of that person;
(b) *Biometric data*: personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of the natural person, which make it possible to clearly identify the person;
(c) *Health data*: personal data relating to the physical or mental state of a natural person, including data on the provision of healthcare services.

Among personal data, in this chapter we focus on personal sensitive data: this is described by the GDPR as a special category of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, […] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[4] It is also worth referring here to the notion of pro-

[3] EU Regulation (EU) 2016/679 of the European Parliament and of the Council—Article 4—Definitions.

[4] EU Regulation (EU) 2016/679 of the European Parliament and of the Council—Article 9—

cessing of personal data. According to the GDPR, processing means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[5] Personal data may be processed by the operator and intermediary as prescribed by law. The GDPR introduces functional requirements, technical requirements, process requirements, privacy requirements through encryption, disaster recovery requirements and also introduces an incident management process. To meet the requirements for processing personal data, the following obligations must be met first:

- *Legality*: fairness and transparency;
- *Transparency* of information: notifications and procedures for exercising the rights of the data subject;
- *Purpose* of processing: exception for research purposes;
- *Processing time*: necessary limitation of data storage must be necessary for the purpose;
- *Data minimization*: data must be accurate and current, and data that is outdated must be erased immediately;
- *Confidentiality and integrity*: protection against unauthorized and unauthorized access and data processing, security of personal data.

Some of the requirements, which companies processing and storing personal data must fulfill, are particularly relevant in the context of IoT. These include monitoring aspects such as IoT vulnerability to various types of hacker attacks, the adopted security measures for IoT and industrial safety, and the review of practices and procedures of business partners (suppliers, customers). At an implementation level, companies also need to take care of the following:

- *Impact assessment of the Internet of Things and data protection*: this obligation is required, in particular, in the case of a new specific personal data processing puts at high risk, if compromised, the rights and freedoms of the person concerned[6];
- *IoT device connectivity*: evaluate the most suitable technological standard and solution for IoT connectivity. These could range from the short-range ones such as ZigBee or those used in a long-range context, such as Low Power Wide Area (LPWA) technologies (e.g., common for smart home solutions and wireless apps);

Processing of special categories of personal data.

[5] EU Regulation (EU) 2016/679 of the European Parliament and of the Council—Article 4—Definitions.

[6] EU Regulation (EU) 2016/679 of the European Parliament and of the Council—Article 34—Data protection impact assessment.

- *Providing consent to the processing of personal data*: informed consent is one of the legal grounds for lawful processing of personal data. Explicit consent by the user is expected also for IoT applications[7];
- *Other GDPR measures relevant to the IoT area*: the GDPR include specific rules on the processing of personal data on children, the right of deletion, the right of access to personal data, or the right to file a complaint with the supervisory authority.[8]

The GDPR does not require special methods to be used for security. Encryption pseudonymization, anonymization, and multifactor authentication are all valid options. Each organization needs to review and choose its methods according to the systems they use, the related costs, and the level of risk.

As described, many of the GDPR requirements are relevant to the IoT. The GDPR regulates specific areas of processing and protection of personal data, not referring to specific technologies. For this reason, the GDPR does not allow addressing with certainty all the issues concerning the IoT. Given the wide scope of the GDPR and general conditions for its compliance, most likely it will be necessary to create, within the GDPR general framework, specific rules and requirements for each relevant IoT area.[9]

The introduction of the GDPR is a step to make the EU the world's lead privacy regulator, in theory a model to be followed worldwide. However, as highlighted by de Arriba-Sellier (2018), there is a concrete risk that the GDPR will empower lawyers, rather than citizens. Risks and challenges are mostly related to the educational (and sociocultural) understanding of the GDPR from companies' communication perspectives, as well as the citizen perspective. To what extent do citizens understand their data protection rights? How will the GDPR affect citizens' smartphone usage practices today? How will it affect the new challenges presented by IoT applications? How big are the differences in privacy perception and experience in terms of age groups, gender, cultures, and lifestyles?

[7] EU Regulation (EU) 2016/679 of the European Parliament and of the Council—Article 6—Lawfulness of processing.

[8] EU Regulation (EU) 2016/679 of the European Parliament and of the Council—Article 12—Transparent information, communication, and modalities for the exercise of the rights of the data subject.

[9] Opinions on specific technologies and application areas have been given by the Article 29 Data Protection Working Party, an independent European advisory body on data protection and privacy set up under Article 29 of the EU Directive 95/46/EC. This advisory board ceased to exist with the entry into force of the GDPR. Throughout the years of work, the Working Party provided opinions on relevant areas such as "apps and smart devices" (WP29, 2013), "Automated individual decision-making and Profiling" (WP29, 2017a) and C-ITS, Cooperative Intelligent Transport Systems (WP29, 2017a).

3 Data Protection in the Context of Connected and Automated Vehicles

Connected and automated driving (CAD) is one of the first IoT application areas that is associated with several entirely new concerns over the personal data protection of transport users and mobility systems. While IoT technologies support the emergence of intelligent transport systems (ITS) delivering an increased level of safety, convenience, and personalization to the user, at the same time they also create conditions for an "always-on," real-time system of global surveillance.

The volume of personal data processed by car manufactures was minimal several years ago. This was mostly related to the information collected through a contract at the time of buying the car, and to the subsequent history of car usage and ownership (e.g., technical maintenance, insurance, change of ownership or residence, and accidents). In the IoT context, thanks to sensors, cameras, and other technological devices (Fig. 1), from which the cars acquire abilities to collect and process information and to interconnect and communicate with transport infrastructure, vehicles, and people inside the car (drivers, passengers) and outside (pedestrians, cyclists). Technically, types of car communications are referred to as Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), and Vehicle-to-Device (V2D). In-car communication can occur, for instance, through various forms of interaction with virtual assistants (Lugano, 2017).

The innovation, development, and use of connected and autonomous vehicles will involve the collection of a wide range of personal data, ranging from transport and mobility data (e.g., location, direction of travel, average speed, mileage, and journey history) to identity and behavioral data (e.g., passengers' identities, car comfort preferences, or health-related data such as fatigue and stress). Even schedules of planned events, collected from passengers' connected devices, may be used for optimizing route and personalized communication.

The short—and largely incomplete—list of types of personal data that may be used in this context is a reason for new privacy concerns, and most likely additional legislative adaptations and requirements. For instance, concerning the purpose of data collection—will such data be collected simply to optimize the travel experience, or will it also be used for targeted marketing, advertising, and profiling (e.g., review of insurance terms based on monitoring of driver's additional health parameters)? From a security viewpoint, what risks would arise from the collection of such data?

As mentioned in the introduction, failure to properly address privacy and security may significantly decrease trust and acceptance toward this new generation of cars, which is already rather low (Abraham et al., 2016; Cavoli et al., 2017; Eurobarometer, 2015, 2017; Kyriakidis, Happee, & De Winter, 2015).

Let us consider the opinion of the Article 29 Data Protection Working Party on C-ITS (WP29, 2017b), "a peer-to-peer solution for the exchange of data between vehicles and other road infrastructural facilities (traffic signs or other transmitting/receiving base stations) without the intervention of a network operator". "[…] Two

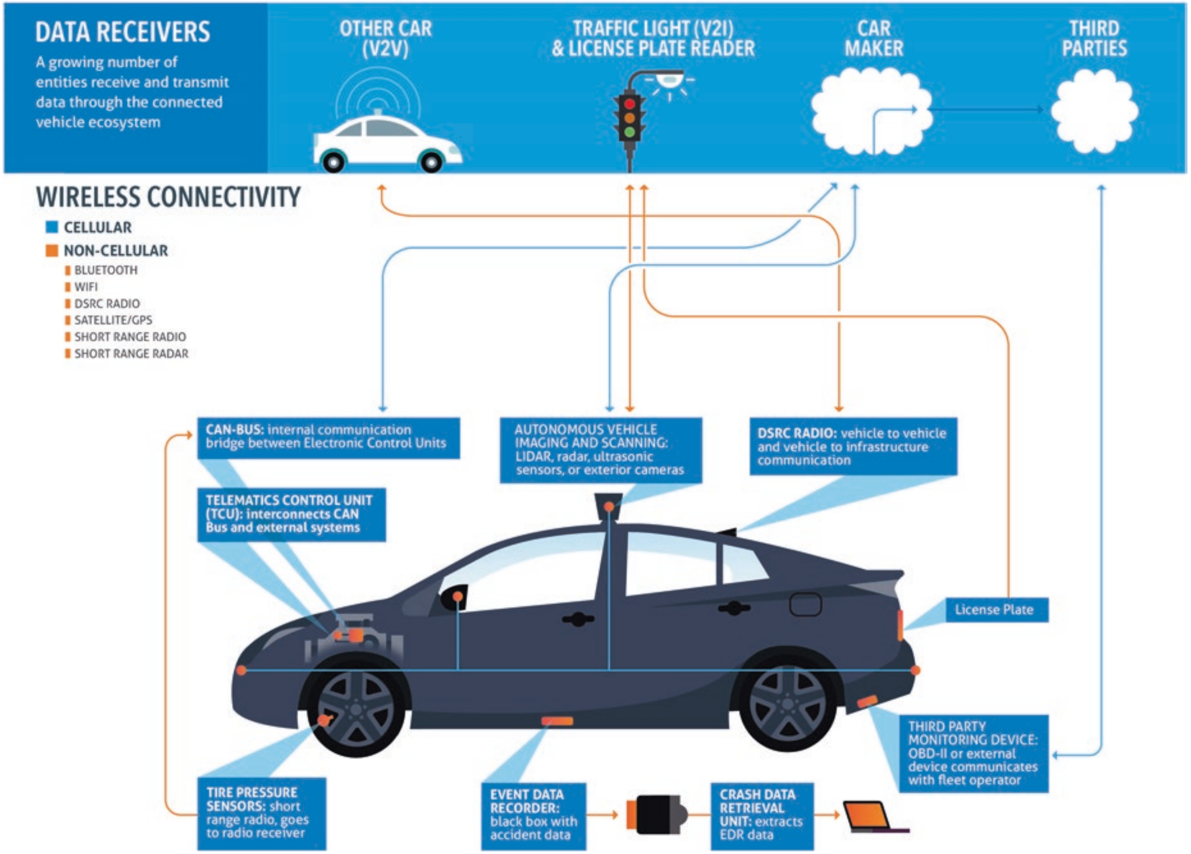

DATA RECEIVERS
A growing number of entities receive and transmit data through the connected vehicle ecosystem
OTHER CAR (V2V)
TRAFFIC LIGHT (V2I) & LICENSE PLATE READER
CAR MAKER
THIRD PARTIES
WIRELESS CONNECTIVITY
CELLULAR
NON-CELLULAR
BLUETOOTH
WIFI
DSRC RADIO
SATELLITE/GPS
SHORT RANGE RADIO
SHORT RANGE RADAR
CAN-BUS: internal communication bridge between Electronic Control Units
AUTONOMOUS VEHICLE IMAGING AND SCANNING: LIDAR, radar, ultrasonic sensors, or exterior cameras
DSRC RADIO: vehicle to vehicle and vehicle to infrastructure communication
TELEMATICS CONTROL UNIT (TCU): interconnects CAN Bus and external systems
License Plate
THIRD PARTY MONITORING DEVICE: OBD-II or external device communicates with fleet operator
TIRE PRESSURE SENSORS: short range radio, goes to radio receiver
EVENT DATA RECORDER: black box with accident data
CRASH DATA RETRIEVAL UNIT: extracts EDR data

Fig. 1 Technologies supporting the connected and automated car (FPF, 2017)

types of messages are exchanged in the context of C-ITS: the so-called Cooperative Awareness Messages (CAM), broadcasted with continuity and containing kinematic data and the dimensions of the vehicle, and the Decentralized Environmental Notification Messages (DENM), sent in addition to the CAM messages only upon the occurrence of specific events (like accidents) for urgent emergency situations, and containing location information about the event." The analysis of the Working Party concluded that broadcast messages exchanged by the vehicles are personal data because they relate to identified or identifiable data subjects. The Working Party also raised specific concerns related to the applicability of GDPR (in particular, Article 11) in the C-ITS context: "By invoking art. 11 of the GDPR without specifying what additional data are necessary to enable identification of the data subjects, the exercise of data subject rights (access, rectification, portability, etc.) is de facto prevented. […] Therefore, the Article 29 Working Party calls for proposals from the C-ITS WG on the concept of "additional information" that can be provided in the context of this new service to make this provision effective, taking into account for instance specific vehicle data, or the highly identifiable nature of location data" (WP29, 2017b).

Additionally, the Working Party also expressed more general privacy concerns about the large-scale deployment of C-ITS. While the variety of benefits of C-ITS introduction are acknowledged, from a privacy perspective, "the large-scale deployment of this new technology, which will entail the collection and processing of unprecedented amounts of location data of individuals in Europe, poses new challenges to the fundamental rights and to the protection of personal data and privacy both of users and of other individuals that will possibly be affected." As an example, C-ITS will share to the cloud information on where people drive and how they drive—information that was previously kept in the mind of the driver or communicated to the GPS of his/her car. The Working Party warns of the fact that "unrestricted and indiscriminate access to data shared within C-ITS may allow for the unfair accumulation of individual movement profiles, a "datification" of driving behaviors, on which personalized goods and services can be shaped, advertised and sold" (WP29, 2017b). Based on the in-depth assessment of the privacy and security risks of C-ITS, a long list of the actions required to enhance the GDPR is provided.

It is worth noting that C-ITS is only one of the technological and application areas of connected and automated driving. For instance, future mobility schemes combining autonomous vehicles with shared mobility typically require some sort of matching between demand and offer, and a degree of service personalization (Krueger, Rashidi, & Rose, 2016). The challenge of data protection can be better understood by referring to the implications related to the continuous collection of one of the key variables, on which the whole connected and autonomous driving ecosystem is built: the tracking of user location by GPS technology. In the USA, the case of *United States v. Jones* attracted broad interest and reflections on the limits of government surveillance and its impact on human rights (Murphy, 2012). In this specific case, the Supreme Court of the United States declared the prolonged GPS tracking of a suspect as unconstitutional, against the Fourth Amendment of the US Constitution.[10] Four weeks of GPR tracking represented a prolonged period, which generated a dossier of about 2000 pages of data including latitude and longitude of the subject's movement. This represented sensitive personal data, as "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations […] Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse" (Jones, 2017).

The "*United States v. Jones*" example is limited to GPR tracking only, but it already gives an idea of the broad data protection implications of these kinds of technologies. In the context of connected and automated driving, large amounts of data will be continuously collected and processed. Joy and Gerla (2017) provide a largely incomplete, but very significant, list of such data:

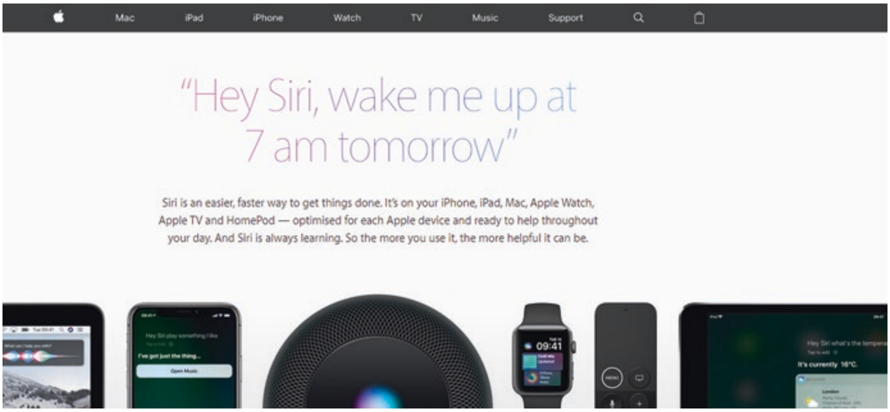
1. External sensors (e.g., GPS, cameras, and lidars);
2. Internal automotive sensors and actuators (e.g., brakes, steering wheel, and accelerator);
3. Internal cockpit sensors (e.g., driver's state of health, alertness, tone of voice, and health sensors like the Ford heart monitor seat);
4. The Driver's messages (e.g., tweets, Facebook, and other crowdsourced info) are also measurable sensor outputs that characterize the state of the system and of the driver;
5. Vehicle's beacons, alarms report on the Vehicle state; say, position, key internal parameters, possible dangers, etc.

While privacy-preserving techniques will be applied, key principles of data protection shall be embedded in the design of the various components of the connected and automated driving ecosystem. To make such a design effective, its implementation should proceed in parallel with the development of an adequate legislative framework (i.e., adaptation of the GDPR, in Europe).

4 Designing Domestic Social Robots for Data Protection

The large-scale deployment of intelligent transport systems, and connected vehicles that are increasingly autonomous, represents just an early sign of many other similar interrelated socio-technical trends. In this section, we describe how social robots, operating as part of intelligent transport systems or in other contexts (e.g., homes, offices, and factories), will grow on an even larger scale of existing data protection challenges.

[10] The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.



"Hey Siri, wake me up at 7 am tomorrow"

Siri is an easier, faster way to get things done. It's on your iPhone, iPad, Mac, Apple Watch, Apple TV and HomePod — optimised for each Apple device and ready to help throughout your day. And Siri is always learning. So the more you use it, the more helpful it can be.

Fig. 2 Presentation of Siri intelligent assistant on Apple website

Social robots, in particular domestic social robots (Esposito, Fortunati, & Lugano, 2014; Fortunati, Esposito, & Lugano, 2015; Vincent, Taipale, Sapio, Lugano, & Fortunati, 2015, Pagallo, 2016), represent another strategic IoT area. There exist several definitions and conceptualizations of a robot: in this chapter, we limit our considerations to robots designed for interacting with humans—thus the concept of social robot—and in a specific interaction context, the domestic environment, i.e., homes. This is what we mean by domestic social robot.

A prominent characteristic of a domestic social robot is its Artificial Intelligence (AI) which is also optimized for interaction with humans. This concerns not only functional interactions and communication but also emotional ones, often in natural language (Baron, 2015; Breazeal, 2003). Although it has been questioned whether intelligent robots need emotion (Pessoa, 2017), it is out of this discussion that social communication is the primary dimension of this type of human–robot interaction (HRI). Within this context, intelligent virtual assistants such as Siri[11] or Google Assistant[12] (Hoy, 2018) are classified as domestic social robots, even if they can be used in any interaction context (i.e., domestic and non-domestic ones). Additionally, they are a form of "intangible" domestic social robot, without a unique physical structure: they can be "hosted" and run on several devices including a smartphone, smart-watch, car communication system, or smart speaker. Unlike "tangible" robots, which are physically located in the domestic context and are not necessarily connected to the IoT, virtual assistants exist in the cloud and are part of the IoT (Fig. 2). This is a key difference, when we analyze them from a data protection point of view.

To further narrow down the context of this analysis, it is best to address robots from the perspective of service robots. This allows differentiating such robots by the type of service or use they are designed for (e.g., companionship and assistance for

[11] https://www.apple.com/uk/ios/siri.

[12] https://assistant.google.com.

the elderly, taking care of domestic tasks, and entertainment). Statistics on service robots are regularly provided by the International Federation of Robotics (IFR). The 2017 IFR report on service robots describes a growing trend of units sold worldwide: while sales of professional service robots remain modest (growth of sales from 48,018 units sold in 2015 to 59,706 sold in 2016), the amount of personal and domestic robots sold worldwide already reaches 6.7 million units, with a market value of 2.6 billion USD (IFR, 2017). Services provided by these robots include vacuum and floor cleaning, lawn-mowing, and entertainment and leisure (e.g., including toy robots, hobby systems, education, and research). In the next 15–20 years, it is expected that the popularity of social robots devoted to elderly and disabled assistance and companionship will increase as one of the measures to alleviate the societal effects of global population aging.

Interacting with domestic social robots reveals a lot about us (Broadbent, 2017). Hence, a key design principle of such robots should be to minimize the potential harm which their collection of personal data could do to the people the robots interact with. In short, domestic social robots should be designed with data protection in mind. This is very challenging, as Pagallo (2016) explains: "Although the claim and goal of lawmakers will probably revolve around the protection of individuals against every harm, e.g., psychological problems related to the interaction with domestic robots and the processing of third parties' information, the intent to embed normative constraints into the internal control architecture of such artificial agents entails a major risk. If there is no need to humanize our robotic applications, we should not robotize human life either."

In this respect, the best possible option would be that domestic social robots are not part of the IoT and the data collected by them is only used within the narrow and well-defined interaction context (i.e., the home). In short, to privilege data protection such robots should not be able to connect to and exchange data with digital networks. In this respect, let us consider the case of a physical domestic robot—the Roomba vacuum cleaner, and the way Google deals with data protection in the context of its intangible virtual assistant.

In relation to Roomba, leader in the production of robotic vacuum cleaners, *The New York Times* in 2017 warned consumers that the maps of their homes, produced and used by Roomba iRobot vacuum cleaners for their cleaning task, may also be uploaded to company servers and potentially sold to other companies such as Amazon, Apple, or Google (Astor, 2017). Although Roomba underlined that the company had no plans to sell such data, they confirmed that this data may be shared for free, with customer consent. In this scenario, homes' maps, clearly identifying a person, may be aggregated with other sources of data concerning that person and used in a variety of ways. Even when not aggregated, information on the size of the apartment and the amount and characteristics of furniture and other equipment can allow estimating owner's income level, and even preferred brands and lifestyle. While it is clear how such information may be used by marketers and advertisers, it is less clear what could be the potential benefits to the customers in sharing such data. Based on the requirements set by the GDPR in Europe, it is also unclear how such requirements could be met by robotic vacuum cleaners, especially in the scenario in which they can exchange data with other IoT apps and devices (belonging to the same user or to other users).

The reasoning behind the Roomba case may be extended to other types of domestic social robots, such as sex robots (Cheok et al., 2017; Danaher & McArthur, 2017; Sharkey et al., 2017). Without entering into any sort of ethical judgment about them, the personal data collected by this kind of domestic social robots would be likely very harmful to the user if such robots are given the possibility to share such data across networks. As to the human–robot emotional and intimate interactions, Calo (2011) warned that "as we manifest these interior reflections of our subconscious, a technology will be recording them. […] they will reveal information about us that a psychotherapist might envy. This arguably novel category of highly personal information could, as any other information, be stolen, sold, or subpoenaed." In 2017, a sex toy company agreed to pay almost four million USD to customers who sued the company in a class action lawsuit. The reason behind the class action was a discovery, by security researchers, that the company was collecting and processing customers' personal data on how customers used the sex toy (e.g., information such as temperature and intensity settings, as well as frequency of use). A Fortune.com story on this case rightly opens the article by stating "Think twice about connecting those sex toys to the Internet."[13] In addition to companies' inappropriate data collection practices, it is likely that without appropriate data protection mechanisms, the aforementioned phenomena of sexting and revenge porn could assume new worrying forms, dramatically impacting people's lives.

In parallel to physical robots and robotic devices, data collected by virtual intelligent assistants must be considered. Think of the data collected by Google Assistant, one of the most advanced and popular examples of this kind of technology:

- *Web and app activity*: this includes online searches and history, and nature of browsed content;
- *Device information*: contents stored on the device such as lists and details of contacts, calendar events, personal notes, and apps;
- *Voice and audio activity*: records voice and audio input.

Additionally, the user may also allow consent for other types of data such as:

- *Screen sharing*: user may allow Assistant to process content that is on the screen of the device (e.g., camera, photo, and document) to provide recommendations and complementary information;
- *Voice match*: voice recognition commands.

In line with Google's Privacy Policy, the collected data "may be used to deliver more useful ads."[14]

The security of intelligent virtual assistants are not receiving sufficient attention (Chung et al., 2017), despite the major risks that they pose to users' assumed per-

[13] Sex toy maker pays $3.75 million to settle 'smart' vibrator lawsuit. Available at http://fortune.com/2017/03/10/sex-toy-maker-settlement-smart-vibrator-lawsuit/.

[14] https://support.google.com/assistant/answer/7126196?p=assistant_privacy&hl=en.

sonal privacy. Courtney (2017) highlighted that “users may need to start censoring what they say, or face the very real prospect of a digital spy leaking more information than they care to divulge.”

While the conversation around connected and automated driving concerns various initiatives around the world aimed at improving the current legislative framework, for the area of domestic social robots—particularly when they are considered as part of the IoT ecosystem—there are many open questions, and the ongoing efforts to regulate this area are too limited.

5 Conclusion

Society is undergoing a major digital transformation affecting all areas of human activity. While the expected benefits of this societal turn are many, the use of IoT technologies presents challenges and risks from the viewpoint of fundamental human rights, such as privacy, that should not be underestimated.

In parallel to technological advancements, the legislative framework is constantly adapting to address these emerging needs. In this respect, the recent introduction of the General Data Protection Regulation (GDPR) in Europe is a milestone toward an enhanced citizens’ data protection. However, the GDPR does have its limitations, both from the viewpoint of its practical applicability and the gray areas, mostly related to specific technologies and applications, which should be addressed with specific complements to the GDPR (e.g., guidelines and recommendations). As Baldini et al. (2018) argued, real improvements will only be possible once the IoT will be driven by ethical design, primarily addressing citizens’ rights and interests. This scenario does not however seem to be reflected in the ongoing IoT developments in specific areas such as connected and automated driving, and domestic social robots. Despite the GDPR, mechanisms allowing citizens to have adequate control over their personal data are still not in place, and the advent of the IoT only increases such challenges.

On the other hand, in the digital era, the whole meaning of privacy has evolved and often takes the form of a decision problem in which the user dynamically evaluates the potential utility and the harm associated to the digital sharing of personal content (Lugano & Saariluoma, 2007). Even if this approach is adopted as the basis for the user’s decision-making, to what extent may potential utility and harm related to digital sharing be assessed with sufficient confidence?

In an increasingly networked and digital world, the solution to personal data protection will not lie in withdrawing from all the opportunities that participation in such a world entails. The cost would be social exclusion and marginalization from such a society. Instead, a massive investment in enabling citizens to critically assess what alternative options (e.g., classic vs robotic vacuum cleaners and traditional vs self-driving cars) mean in terms of personal privacy is strongly needed. Although this is a key responsibility of the public sector, educational systems, and families, the private sector should be held accountable in the co-creation of an IoT that is as trustworthy as the companies and organizations behind it. In this context, the research community has a central role, as the knowledge produced should be used both for evidence-based decision-making and for fine-tuning and calibrating IoT design and applications.

An important lesson was learned from the case studies on connected and automated driving and domestic social robots. If these developments are necessary for society, it is clear that their functionality is largely based on the collection and processing of variables that are considered personal data and personal sensitive data. From the user perspective, such data is used in a specific context (e.g., matching demand and offer in a shared mobility system with autonomous vehicles). Being its usefulness is limited in time, it would be desirable to have an "expiration date" for the collected data. After that, no trace of such data would exist in the cloud. Potential renewal in the processing of such data should be explicitly provided by the user. This solution, however, would not allow an intelligent system to learn, since this learning is based on the processing of large amounts of data. The trade-off here is therefore on a suitable "expiration period" that would still allow the system to learn. Additionally, technical solutions are needed to avoid the indiscriminate duplication and sharing of personal data. Data anonymization is important, but not sufficient as there are known techniques with de-anonymizing data (Su, Shukla, Goel, & Narayanan, 2017). Finally, for the specific domestic context it may be more desirable for citizens' privacy that only a few of their belongings get "smart" and "connected" to the IoT.

Acknowledgements The article was published with the support of the project ERAdiate—Enhancing Research and innovAtion dimensions of the University of Žilina in intelligent transport systems, co-funded from European Union's Seventh Framework Programme for research, technological development, and demonstration under grant agreement no. 621386.

References

Abraham, H., Lee, C., Brady, S., Fitzgerald, C., Mehler, B., Reimer, B., & Coughlin, J. F. (2016). *Autonomous vehicles, trust, and driving alternatives: A survey of consumer preferences. White paper 2016-6*. Cambridge, MA: MIT AgeLab.

Agarwal, R., Gao, G., DesRoches, C., & Jha, A. K. (2010). Research commentary—The digital transformation of healthcare: Current status and the road ahead. *Information Systems Research, 21*(4), 796–809.

Astor, M. (2017, June 25). Your Roomba may be mapping your home, collecting data that could be shared. *The New York Times*. Retrieved from www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical design in the internet of things. *Science and Engineering Ethics, 24*(3), 905–925.

Baron, N. S. (2015). Shall we talk? Conversing with humans and robots. *The Information Society, 31*(3), 257–264.

Bounfour, A. (2016). *Digital futures, digital transformation*. Cham, Switzerland: Springer.

Breazeal, C. (2003). Emotion and sociable humanoid robots. *International Journal of Human-Computer Studies, 59*(1–2), 119–155.

Broadbent, E. (2017). Interactions with robots: The truths we reveal about ourselves. *Annual Review of Psychology, 68*, 627–652.

Calo, M. R. (2011). Robots and privacy. In P. Lin, K. Abney, & G. A. Bekey (Eds.), *Robot ethics: The ethical and social implications of robotics* (p. 187). Cambridge, MA: MIT Press.

Cavoli, C., et al. (2017). *Social and behavioural questions associated with automated vehicles. A literature review*. London, UK: Department for Transport.

Cheok, A. D., Levy, D., Karunanayaka, K., & Morisawa, Y. (2017). Love and sex with robots. In *Handbook of digital games and entertainment technologies* (pp. 833–858). Singapore: Springer.

Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). Alexa, can I trust you?. Computer, 50(9), 100–104.

Courtney, M. (2017). Careless talk costs privacy [digital assistants]. *Engineering & Technology, 12*(10), 50–53.

Danaher, J., & McArthur, N. (Eds.). (2017). *Robot sex: Social and ethical implications*. Cambridge, MA: MIT Press.

de Arriba-Sellier, N. (2018, June 5). GDPR: the risks of empowering lawyers, not citizens. *Leiden Law Blog*. Retrieved from http://leidenlawblog.nl/articles/gdpr-the-risks-of-empowering-lawyers-not-citizens

Duportail, J. (2017, September 26). I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold

Englander, E. K. (2015). Coerced sexting and revenge porn among teens. *Bullying, Teen Aggression & Social Media, 1*(2), 19–21.

Esposito, A., Fortunati, L., & Lugano, G. (2014). Modeling emotion, behavior and context in socially believable robots and ICT interfaces. *Cognitive Computation, 6*(4), 623–627.

Eurobarometer. (2015). *Special Eurobarometer 427: Autonomous systems*. European Commission. https://doi.org/10.2759/413916.

Eurobarometer. (2017). *Attitudes towards the impact of digitalisation and automation on daily life. Report 460*. European Commission. https://doi.org/10.2759/25616.

Fortunati, L., Esposito, A., & Lugano, G. (2015). Introduction to the special issue "Beyond industrial robotics: Social robots entering public and domestic spheres". *The Information Society, 31*(3), 229–236.

FPF. (2017). Data and the connected car. Future Privacy Forum (FPF) Infographic (Version 1.0). Retrieved from https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

Gross, M. (2018). Watching two billion people. *Current Biology, 28*(9), 527–530.

Harmon, R. R., Castro-Leon, E. G., & Bhide, S. (2015). Smart cities and the internet of things. In *2015 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 485–494). IEEE.

Herrmann, M., Boehme, P., Mondritzki, T., Ehlers, J. P., Kavadias, S., & Truebel, H. (2018). Digital transformation and disruption of the health care sector: Internet-based observational study. *Journal of Medical Internet Research, 20*(3), e104.

Hobbs, M., Owen, S., & Gerber, L. (2017). Liquid love? Dating apps, sex, relationships and the digital transformation of intimacy. *Journal of Sociology, 53*(2), 271–284.

Hoy, M. B. (2018). Alexa, Siri, Cortana, and more: An introduction to voice assistants. *Medical Reference Services Quarterly, 37*(1), 81–88.

Hung, M. (2017). *Leading the IoT. Gartner insights on how to lead in a connected world*. Gartner. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

IFR. (2017). *World robotics 2017 service robots report. Executive summary*. Retrieved from https://ifr.org/downloads/press/Executive_Summary_WR_Service_Robots_2017_1.pdf

Jones, A. (2017). Autonomous cars: Navigating the patchwork of data privacy laws that could impact the industry. *Catholic University Journal of Law and Technology, 25*(1), 6.

Joy, J., & Gerla, M. (2017). Internet of vehicles and autonomous connected car-privacy and security issues. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1–9). IEEE.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122.

Krueger, R., Rashidi, T. H., & Rose, J. M. (2016). Preferences for shared autonomous vehicles. *Transportation Research Part C: Emerging Technologies, 69*, 343–355.

Kyriakidis, M., Happee, R., & De Winter, J. C. F. (2015). Public opinion on automated driving: Results of an international questionnaire among 5,000 respondents. *Transportation Research Part F: Traffic Psychology and Behaviour, 32*, 127–140.

Lugano, G. (2010). *Digital community design: Exploring the role of mobile social software in the process of digital convergence* (253p). Jyväskylä studies in computing, 114. Jyväskylä: University of Jyväskylä.

Lugano, G. (2017, May). Virtual assistants and self-driving cars. In *ITS Telecommunications (ITST), 2017 15th International Conference on* (pp. 1–5). IEEE.

Lugano, G., & Saariluoma, P. (2007, July). To share or not to share: Supporting the user decision in mobile social software applications. In *International conference on user modeling* (pp. 440–444). Berlin, Germany: Springer.

McNeal, R. S., & Schmeida, M. (2015). Digital paranoia: Unfriendly social media climate affecting social networking activities. In *Social media and the transformation of interaction in society* (pp. 210–227). Hershey, PA: IGI Global.

Miksch, L., & Schulz, C. (2018). *Disconnect to reconnect: The phenomenon of digital detox as a reaction to technology overload*. Lund, Sweden: Master's Program in International Marketing and Brand Management, Lund University.

Murphy, E. (2012). Back to the future: The curious case of United States v. Jones. *Ohio State Journal of Criminal Law, 10*, 325.

Nandwani, M., & Kaushal, R. (2017, July). Evaluating user vulnerability to privacy disclosures over online dating platforms. In *International conference on innovative mobile and internet services in ubiquitous computing* (pp. 342–353). Cham, Switzerland: Springer.

Newman, A. L. (2015). What the "right to be forgotten" means for privacy in a digital age. *Science, 347*(6221), 507–508.

Pagallo, U. (2016). The impact of domestic robots on privacy and data protection, and the troubles with legal regulation by design. In Data protection on the move (pp. 387–410). Springer, Dordrecht.

Panel, I. C. T. (2002). *Digital transformation: A framework for ICT literacy*. Princeton, NJ: Educational Testing Service.

Pessoa, L. (2017). Do intelligent robots need emotion? *Trends in Cognitive Sciences, 21*(11), 817–819.

Salem, F. (2016, February 10). *Smart city for public value: Digital transformation through agile governance—The case of 'Smart Dubai'*. World Government Summit Publications, Forthcoming. Retrieved from https://ssrn.com/abstract=2733632

Seufert, S., & Meier, C. (2016). From eLearning to digital transformation: A framework and implications for L&D. *International Journal of Advanced Corporate Learning (iJAC), 9*(2), 27–33.

Sharkey, N., van Wynsberghe, A., Robbins, S., & Hancock, E. (2017). *Our sexual future with robots*. The Hague, Netherlands: Foundation for Responsible Robotics. Retrieved from http://responsiblerobotics.org/wp-content/uploads/2017/07/FRR-Consultation-Report-Our-Sexual-Future-with-robots_Final.pdf

Su, J., Shukla, A., Goel, S., & Narayanan, A. (2017, April). De-anonymizing web browsing data with social networks. In *Proceedings of the 26th international conference on world wide web* (pp. 1261–1269). Geneva, Switzerland: International World Wide Web Conferences Steering Committee.

Taipale, S. (2009). *Transformative technologies, spatial changes. Essays on mobile phones and the Internet* (PhD dissertation). University of Jyväskylä, Jyväskylä.

Ugur, N. G., & Koc, T. (2015). Time for digital detox: Misuse of mobile technology and phubbing. *Procedia-Social and Behavioral Sciences, 195*, 1022–1031.

Vincent, J., Taipale, S., Sapio, B., Lugano, G., & Fortunati, L. (Eds.). (2015). *Social robots from a human perspective*. Berlin, Germany: Springer.

Wajcman, J. (2015). *Pressed for time: The acceleration of life in digital capitalism*. Chicago, IL: University of Chicago Press.

Weber, R. H. (2010). Internet of things–new security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30.

WP29. (2013). *Opinion 02/2013 on apps on smart devices*. 00461/13/EN WP 202. Article 29 Data Protection Working Party. Adopted on 27 February 2013.

WP29. (2017a). *Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679*. 17/EN WP251rev.01. Article 29 Data Protection Working Party. Last revised and adopted on 6 February 2018.

WP29. (2017b). *Opinion 03/2017 on processing personal data in the context of cooperative intelligent transport systems (C-ITS)*. 17/EN WP 252. Article 29 Data Protection Working Party. Adopted on 4 October 2017.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal, 4*(5), 1250–1258.