# The Smart World Revolution

Eleni Kosta[1](✉), Igor Nai Fovino[2], Simone Fischer-Hübner[3], Marit Hansen[5], Charles Raab[4], Ignacio Sanchez[2], and Diane Whitehouse[6]

[1] Tilburg Institute for Law, Technology, and Society (TILT), Tilburg Law School, 90153, 5000LE Tilburg, The Netherlands
e.kosta@tilburguniversity.edu

[2] European Commission, Joint Research Centre (JRC), Directorate for Space, Security and Migration, Cyber and Digital Citizens' Security Unit, Via E. Fermi 2749, 21027 Ispra, VA, Italy
{igor.nai-fovino,ignacio.sanchez}@ec.europa.eu

[3] Department of Computer Science, Karlstad University, Universitetsgatan 2, 65188 Karlstad, Sweden
simone.fischer-huebner@kau.se

[4] Politics and International Relations, School of Social and Political Science, University of Edinburgh, Chrystal Macmillan Building, 15a George Square, Edinburgh EH8 9LD, Scotland, UK
c.d.raab@ed.ac.uk

[5] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstr. 98, 24103 Kiel, Germany
marit.hansen@privacyresearch.eu

[6] The Castlegate Consultancy, 27 Castlegate, Malton, UK
diane.whitehouse@thecastlegateconsultancy.com

**Abstract.** The explosion of the phenomenon of the Internet of Things and the increasing diffusion of smart living technologies in all the layers of our society – from houses to hospitals, from cities to critical infrastructures such as energy grids – clearly demonstrates the viability and the advantages of a fully interconnected vision of a smart world. Technological advances such as the use of open data, big data, blockchain and sensor development in the Internet of Everything are rapidly changing the societal landscape, raising the question of how to guarantee, in a homogeneous way, the preservation of privacy and other human rights in a completely heterogeneous and cross-sectoral world, without impairing the potentialities of the new smart technologies such as the Internet of Things and big data. The 2017 IFIP Summer School on Privacy and Identity Management was dedicated to the exploration of technical, legal and societal issues relating to the smart revolution. This chapter provides an introduction to the exciting work presented at the summer school.

**Keywords:** Smart revolution · Summer school · Privacy · Data protection

M. Hansen et al. (Eds.): Privacy and Identity 2017, IFIP AICT 526, pp. 3–12, 2018.
https://doi.org/10.1007/978-3-319-92925-5_1

## 1 An Introduction to the Summer School on the Smart World Revolution

The world is in the throes of a 'smart' revolution. From smart watches, to smart cars and from smart TV to smart robots, technological developments foster a wide range of smart applications and devices. Digital data is an essential resource for economic growth, competitiveness, innovation, job creation, and societal progress. To be exploited, data needs to flow across borders and sectors. It should be smartly aggregated and should be accessible and reusable by most stakeholders. The explosion of the phenomenon of the Internet of Things and the increasing diffusion of smart living technologies in all the layers of our society – from houses to hospitals, from cities to critical infrastructures such as energy grids – clearly demonstrates the viability and the advantages of a fully interconnected smart world. However, this vision poses concrete concerns related to the potential antagonism between the 'trend to share everything' on the one hand, and the 'citizen's right to privacy and security', on the other. Dilemmas concerning opportunities for discrimination, social profiling, and social exclusion also arise.

The European framework on data protection has been recently reformed. The European Union (EU) General Data Protection Regulation (GDPR)[1] replaces the 1995 Data Protection Directive[2] and becomes applicable as of May 2018, providing an overarching legislative framework that responds to the concerns of processing personal data. Parallel to the adoption of the GDPR, a new Directive was adopted to protect personal data processed for the purpose of criminal law enforcement (LED)[3]. The 2002 e-Privacy Directive[4] regulates issues relating to privacy and data protection in relation to electronic communications services offered over public communications networks. In January 2017, the European Commission published a proposal[5] for the revision of

[1] European Parliament and the Council of the European Union, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L 119/1 (4.5.2016).

[2] European Parliament and the Council of the European Union, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (23.11.1995).

[3] European Parliament and the Council of the European Union, Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89 (4.5.2016).

[4] European Parliament and the Council of the European Union, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 (31.07.2002).

[5] European Commission, Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) {COM(2017) 10 final}.

that Directive as well. The Commission proposed the replacement of the Directive by a Regulation that may eventually provide an instrument to enforce not only the privacy, but also, to some extent, the security of the upper layers of the telecommunication services relevant for implementing a smartly interconnected world. One of the novelties of the proposed e-Privacy Regulation is the extension of its scope to include new functionally equivalent electronic communications services offered by Over The Top (OTT) players i.e., with no involvement of multi-system operators. The goal of the expansion of the scope of the Regulation to OTTs is to ensure respect for the principle of confidentiality and the protection of fundamental rights in those types of services[6].

While these legislative instruments define the principles to be respected and enforced, not a lot has been said about the *way* in which these principles should be deployed technically in different industrial and societal sectors. Technological advances such as the use of open data, big data, blockchain and sensor development in the Internet of Everything are rapidly changing the societal landscape. Questions arise about who holds what data, and where and how that data may be used. These advances challenge the way in which privacy and data protection should be handled, because current national regulatory mechanisms were not devised with these new technologies and possibilities in mind. What is also clear, from discussions in the general press, media and social media, is that there are also huge societal, social, and ethical concerns with regard to the implications of these emerging technologies both in theory and in their practical deployment.

Here, indeed, lies a major scientific and social challenge: how to guarantee, in a homogeneous way, the preservation of privacy and other human rights in a completely heterogeneous and cross-sectoral world, without impairing the potentialities of the new smart technologies such as the Internet of Things and big data. Such questions, as well as many other current and general research issues surrounding privacy and identity management, were addressed by the 2017 IFIP Summer School on Privacy and Identity Management.

The Summer School welcomed contributions from PhD students from various disciplines (e.g., computer science, informatics, economics, ethics, law, psychology, sociology, history, political and other social sciences, surveillance studies, business and public management). These contributions were supplemented by invited talks from experts in the field, as well as tutorials and workshops. This volume reflects the outcome of the exciting work presented at the summer school and mirrors the sparkling interdisciplinary debates that took place during and around the event. The submissions are divided into six categories, each dealing with a concrete aspect of the 'smart revolution': privacy engineering, privacy in the era of smart revolution, improving privacy and security in the era of smart environments, safeguarding personal data and mitigating risks, assistive robots, and finally, mobility and privacy.

[6] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.1.2017 COM(2017) 10 final, p. 4.

## 2 Privacy Engineering

Privacy engineering is a key topic that aims at the development of methodologies, tools and techniques that contribute to ensuring privacy in engineered systems. Given the importance of privacy engineering in the era of 'smart revolution', the Summer School organisers invited three groups of distinguished researchers to cover various aspects of this topic.

Privacy and data protection by design are important principles embraced by the privacy and data protection community: they were recently captured in the content of the GDPR. The notion of "by design" implies that the privacy and data protection dimension should be considered at the inception of new projects and taken into account all the way during the projects' design and development.

In Chap. 2, Del Alamo, Martín and Caiza, in their invited paper, provide an introduction to the emerging field of privacy engineering, which aims to bridge the gaps among the legal, the academic and the engineering dimensions with the goal of providing engineers with tools and methods to address data protection and privacy during the software development process. In this work, the authors describe a conceptual metamodel that can be used to organise and structure knowledge in this domain in a way that can be more easily used and integrated into engineering practice. They elaborate on privacy design patterns as means to gather systematic reusable knowledge.

The topic of data protection by design is also at the core of the chapter authored by Rommetveit, Tanas and van Dijk. This invited paper presents results from recent empirical investigations on privacy by design and privacy engineering (the H2020 CANDID project), in which social science methods such as written consultations, questionnaires, interviews and focus groups were used to research the existing approaches, perceptions, imaginations and expectations in regard to privacy engineering. Tensions and frictions discovered during these investigations are described in the chapter, such as lessons learnt relating to the limits of privacy by design that should not be passed – the impossibility of "law becoming code" in the strict sense of the word.

In Chap. 4, Marx, Sy, Burkert, and Federrath focus on the heavily debated issue of ensuring anonymity in the online world. Their contribution starts with an overview of relevant terminology particularly in the field of computer science, points to data protection regulation on the European level, and shows their work on formalising anonymity. Furthermore, the authors give an overview of different techniques and solutions providing anonymity on the application level as well as on the network level, protecting against adversaries of different strengths. They conclude that the protection of users' privacy on the Internet becomes increasingly difficult and discuss risks such as those involved in fingerprinting as well as storage-based and behaviour-based tracking. Finally, they identify open research questions, in particular with respect to practical and usable anonymity on the Internet.

## 3 Privacy in the Era of the Smart Revolution

Issues revolving around conceptualisation of privacy and principles relating to privacy protection could not but be in the focus of numerous contributions to the Summer School. The increased popularity of interconnected devices puts privacy and data protection at the centre of the cyber-arena even more than in the past. However, the debate is not only around technologies, but also around their users and how they perceive privacy.

Kitkowska, Wastlund, Meyer and Martucci performed an empirical investigation on the perception of privacy harm. In their work they identify differences in privacy concerns related to information disclosure, protection behaviour and demographics. Additionally, their results suggest that there are some general tendencies in privacy concerns. Their findings show that people create simplified models of privacy harms, such as worries about security, unlawful use of data, disclosure or exposure.

Three co-authors (Patrignani, Whitehouse and Gemo) investigate the changes that have taken place in the concept of privacy, due to both societal and technological advances, based on a 1999 consideration that one should forget about data privacy. This topic was discussed during one of the workshops held at the Summer School, through the prism of disciplines such as ethics, philosophy, and education. The goal of the workshop was to stimulate reflection and discussion among attendees by assessing a broad set of questions. Examples follow: Is privacy still a human right? What are the implications of data collection and the cloud for privacy? What will become of the concept of privacy in the future? What kinds of education will be needed in the future to inform children and young people particularly about notions of privacy and future technological developments? Each of four main questions/topics are handled, analysed and discussed in a separate section of Chap. 6. The co-authors then lay out tentative conclusions, emerging both from and after the workshop.

In their invited paper, Sabelli and Tallacchini approach the principle of fairness as a core principle in privacy protection in the era of algorithms and big data. The authors provide an overview of the historical evolutions of privacy legislation in the United States (US) and the European Union (EU). They further discuss how the legal and ethical debates on the digital world in the two continents have significantly opened up to include new dimensions other than privacy, particularly in connection with machine learning algorithms and big data. While acknowledging that privacy and data protection remain essential interpretive constructs in the information and communication technology (ICT) domain, they can no longer be seen as capable of capturing all relevant normative issues in the digital space. Issues of discrimination, equal opportunity, fairness and, more broadly, models of justice, are gradually entering the picture, requiring novel approaches. The authors offer concrete examples of the inadequacy of privacy and data protection to cover new normative concerns related to big data and machine learning, such as the broadly known anti-spam filters. According to the authors, however, attempts to grant algorithmic fairness represent just the first step in solving new digital normative issues. The wider question about what models of justice people are willing to take into account and apply still needs to be addressed.

The topic of the next chapter is closely related to the general question about fairness and the role of individuals. Consent – what it means, how it can be implemented, what part it plays in legitimising data processing – is a central topic and focus of debate in the communities of scholars, regulators and practitioners of data protection. Whether it is possible for consent to be 'freely given, specific, informed and unambiguous' (GDPR, Art. 11(4)) in all the contexts in which it is sought engages many complex forms of behaviour in terms of law, communication processes, cognitive processes and power relationships that provide the conditions that must be satisfied if consent is to be more than a rhetorical or ideological gesture in the idiom of informational self-determination. Bergemann's discussion is timely and contributes to an understanding of consent by examining a large body of existing literature and exploring what he calls the 'consent paradox': 'How can we account for the prominent position of consent despite critique?'. This is set within the long-running German debate about consent, which the author analyses using the tools of discourse analysis rather than those of philosophy and law. He casts light on how the 'paradox' is sustained through the very critique of consent, and not despite it. The critique emphasises the larger social issues and conflicts that come to the fore in and around the idea and practice of consent across many fields of data processing. His conclusion points to a rethinking of data protection in terms of a more comprehensive critique of power.

The notion of the Internet of Things has gained in prominence, reaching public attention over the past decade. Devices are now on the market and are being increasingly used. In Chap. 9, Railean and Reinhardt conduct a questionnaire survey on Internet of Things products: their acquisition, use and eventual discarding/ de-commissioning, and the implications that these three activities have for privacy. Implicit in the authors' investigation of the devices – many of which may be embedded or hidden – is a lifecycle approach. This chapter raises concerns with regard to 'digital literacy' or, perhaps, the 'privacy literacy', of people in contemporary society, especially users who – for various reasons – may be relatively vulnerable. The end focus of the paper is, however, on a set of nine recommendations made to the vendors of Internet of Things devices, which may individually or collectively improve the companies' privacy practices. Replication of the work by the same (or different) researchers in other settings and/or on the larger scale than the 110 completed responses achieved by this research may be encouraged by the fact that the 30+ survey questions are laid out in an annex to the paper.

## 4 Improving Privacy and Security in the Era of Smart Environments

The third set of contributions aimed at proposing solutions or approaches that will contribute to the improvement of privacy and security.

Chapter 10 summarises the workshop that two H2020 projects jointly held at the Summer School: the CREDENTIAL project and the PRISMACLOUD project. Both projects employ cryptographic primitives for cloud services that aim at improving security and privacy features. The workshop organisers presented several concepts and pilots of privacy-preserving solutions that enable storing, sharing, and processing of potentially sensitive data in untrusted clouds environments. The vivid discussion that followed encompassed junior and senior researchers from multiple disciplines and resulted in some new aspects that may help the further evolution of the concepts and implementations as well as ways to demonstrate their advantages.

Sakpere and Kayem address, in Chap. 11, the need for re-designing existing applications under privacy-based-service-oriented principles. In particular, in their paper, they present a solution for anonymising streaming crime data using k-anonymity, l-diversity and t-closeness approaches.

In line with some of the considerations that motivated the previous work, Shulman, with a completely different approach, argues that to address privacy-related decisions it is necessary to consider aspects of human cognition, employing, for instance, methods used in Human-Computer Interaction (HCI) and Information Science research. In his contribution, Shulman analyses findings and contributions of existing privacy decision-making research and suggests filling gaps in current understanding by applying a cognitive architecture framework to model privacy decision-making.

## 5 Safeguarding Personal Data and Mitigating Risks

Closely linked to the previous session of the school are contributions that focus on the safeguarding of personal data and the mitigation of risk, especially in view of the new principles and rights introduced in the GDPR.

In Chap. 13, Bieker, Martin, Friedewald and Hansen report on their interactive workshop that dealt with Data Protection Impact Assessment (DPIA), which plays an important part in the GDPR as an instrument for assessing and mitigating data processing's potential risk to rights and freedoms. DPIA builds on decades of practice that was shaped around Privacy Impact Assessment (PIA), of which there have been many varieties and levels of quality around the world. The GDPR, however, is unclear about what is expected in a DPIA, and how to perform it, although it is mandatory in many cases. The workshop aimed to enable participants to become more familiar with DPIA, how it can be carried out, and what issues are likely to arise in this process. It did this through expounding a diagrammatic Standard Data Protection Model, explaining the inventory of data protection goals derived from legal requirements, and involving the workshop attendees in examining two case studies in terms of risks to rights and freedoms: smart surveillance in train stations, and emotional coding for in-store advertising. The authors conclude that more research and refinement is needed to improve the ability to implement DPIA in complying with the GDPR, and that a multidisciplinary perspective is required to identify and mitigate risks.

In Chap. 14, Raschke, Küpper, Drozd and Kirrane focus on designing a GDPR-compliant and Usable Privacy Dashboard. The chapter outlines the design, implementation and first expert user evaluation of a Privacy Dashboard that was developed in the scope of the EU H2020 project, SPECIAL, for enabling data subjects to exercise their data subject rights in compliance with the GDPR. A specific focus, in contrast to previous related work on privacy dashboards, is on consent review and withdrawal.

Neisse, Steri and Nai Fovino provided an invited contribution in the form of an extended abstract on blockchain-based identity management and data usage control. The authors discuss the approach for a blockchain-based solution based on smart contracts, which helps to enforce the transparency and accountability principles of the GDPR. In particular, their solution allows end users to track how their data were processed by data controllers and data processors and whether the processing of their data is compliant with their provided consent. Controllers and processors can in turn prove that they have rightfully obtained consent and are not violating data protection obligations. Three different solutions for provenance and accountability tracking models using blockchains are analysed and compared in regard to privacy, performance and scalability.

The invited extended abstract of Ferrari follows, focusing on Identification Services for Online Social Networks (OSNs). Given that digital identities are a key element of OSNs, their users become more reliant on online identities with often no means of knowing who really is behind an online profile. The problem of fake accounts and identity-related attacks in OSNs has attracted considerable interest from the research community. In her short paper, Ferrari provides an overview of the Sybil attack problem, briefly discussing the research proposals aimed at empowering users with tools that can help them to identify the validity of the online accounts with which they interact.

Chapter 17 summarises a workshop given at the Summer School on a design and reporting toolkit for experimental HCI research related to privacy and cyber security that was presented and practically applied to exemplary publications. Coopamootoo and Gross present a set of ‘completeness indicators’ for the quality of experimental research that can support researchers in the design phase of a user study and provide a structure for writing and reviewing research papers in that area.

## 6 Assistive Robots

A book on today’s ‘smart revolution’ would be incomplete without contributions on robots and their ethical implications.

Based in Germany, Heuer, Schiering and Gerndt have begun to explore some of the ethical concerns, especially around privacy, implied by the use of socially assistive robots. Their almost 60-item literature search – a meta-study – has permitted them to structure the problem area. Not only did the authors categorise socially assistive robots into four types – ranging from the more functional to the most human-like – but they also explored how three categories of users – children, families, and older adults – might experience privacy concerns. Ultimately, their research shows that relatively little attention has been paid to date to the ethics of socially assistive robots. This conclusion appears especially surprising when one considers the vulnerability of the parties involved. The ethics of robot design and robot use is clearly a domain to watch. One should anticipate more in-depth investigations of the ethical, social, and societal implications of robot use in a range of fields, especially over the life-course of human beings.

In Chap. 19, De Conca presents a theoretical model called the Aggregated Privateness Model, inspired by the structure of snowflakes, to explain a change in the 'positioning' of the home with regard to its role as place of expression and protection of the private sphere. The change is connected to the presence of robotic intelligent assistants such as Google Home and Amazon Echo inside the home, and in particular with the constant fluxes transferring information in and out of the private sphere. The data collected and transferred by such devices creates several detailed profiles and predictive models that overlap with the individuals inside the home, creating an entire informational ecosystem around them while maintaining certain aspects of 'privateness' and seclusion. This projects the home and the private spheres of individuals into a dense informational structure, a hive of data (described by De Conca's model as an interaction of clusters of nodes and aggregates of privateness) whose connections spread in different directions. In this way, De Conca's model sheds light on a more collective dimension of privacy, a context in which mathematical rules gain normativity. The model highlights how the behaviour of individuals can influence the other private spheres in the clusters and the aggregation itself due to a network effect, and how Diffused Network Liability could help compensate for such influences without becoming practically impossible.

## 7 Mobility and Privacy

It has been more than 20 years since mobile phones became an integral part of the everyday life of individuals, a phenomenon that intensified with the introduction and exponential growth of smartphone devices. This collection of chapters on mobility and privacy contains texts that are focused on mobile phones and the vast capabilities they offer.

Kununka, Mehandjiev and Sampaio present the results of a study in which they analyse the privacy policies of a dataset of Android and IOS apps to determine to what extent these policies reflect the actual behaviour of the apps in terms of collection and flows of personal data to third parties. Their results show that there are a substantial numbers of apps, both in Android and IOS, that collect, manage and disseminate personal data in a way that does not match the description and requirements provided in their privacy policies. These results highlight the need to put in place mechanisms to ensure the enforcement of privacy policies and secure their alignment with the actual behaviour of the apps. The authors suggest that privacy policy specification languages could be used for the automatic enforcement of privacy policies, facilitating the development of technological solutions that could assist in the monitoring of the compliance of apps with their policies and the provision of an opt-out for users in cases of non-compliance.

In their paper, Harborth and Pape examine the privacy-related behaviour of players of Pokémon Go – a location-based augmented reality game available on mobile phones – in Germany. The two researchers have conducted an online two-part survey to study both the attitudes and the behaviour of players. Their focus is chiefly around the privacy paradox. They examine the extent to which players express their concerns about privacy and whether they then behave in a privacy-preserving way. Three highlights of the paper are: the examination of the differences in attitude/behaviour dependent on the age and the gender of the Pokémon Go players; the wealth of the literature explored; and the availability of the survey questions in an annex. As a result, other researchers may be tempted to replicate the study in different cultural settings and with the same (or extended) augmented reality applications. Will the dilemmas surrounding the gap between expressed concern and actual behaviour remain? And will utilitarian trade-offs continue?

Data processing in the health sector is based on sensitive data. It is of the utmost importance that privacy risks are detected and mitigated. This is the starting point for the contribution from Gabel, Schiering, Müller and Ertas. The authors focus on mobile health applications and analyse the scenario of neuropsychological training after brain injuries. Employing privacy protection goals and privacy design strategies, they model privacy requirements such as the pseudonymity of patients, data minimisation and transparency. Finally, the authors suggest technical and organisational measures to implement those requirements.

Near Field Communication (NFC) is being used for payments. In the contribution from Kumar, Bechinie and Tscheligi, the authors investigate the gaps between user perception and reality, in particular concerning privacy and security aspects. They conducted a study that showed that users have different mental models about NFC. The authors propose to modify NFC payment systems in such a way that users can gain experience not only in their usage, but also better understand privacy and security concepts.

In Chap. 24, digital identities are discussed as a key element of the future digital society. Today there is already a broad range of existing electronic identity (eID) systems, which provide methods to sign documents or authenticate online services. Quite often, however, these identities lack appropriate techniques so that they can be used as regular identity cards to digitally authenticate an eID holder to a physical person in the real world. Starting from this assumption, Hölzl, Roland and Mayrhofer explore a new way of implementing mobile eID taking into consideration this requirement in a privacy-preserving fashion.

## 8 Outlook to the Future

The annual IFIP Summer Schools offer a wonderful platform for PhD students and experienced researchers alike, to present their work and to benefit from the exchange and cross-fertilisation of ideas during an intensive week of lectures, presentations, tutorials and workshops. The contributions to the 2017 IFIP Summer School that were presented either as PhD papers, invited talks or workshops, all cover different aspects of privacy and security in the era of the smart revolution: from privacy engineering to risk mitigation and from assistive robots to mobile applications.

The 2017 IFIP Summer School offered an exciting journey through the challenges that are raised by recent technological developments and the rethinking and novel conceptualisations of traditional issues in the scholarly debates on privacy and identity management. It is our aspiration that research in this field will continue, and that answers to some of the questions that were raised during the Summer School and that are included in chapters of this volume will be answered in the coming years. And – why not? – maybe in one of the following IFIP Summer Schools.