Public Administration and Information Technology 30

J. Ramon Gil-Garcia
Theresa A. Pardo
Mila Gasco-Hernandez *Editors*

Beyond Smart and Connected Governments

Sensors and the Internet of Things in the Public Sector

Springer

Public Administration and Information Technology

Volume 30

Series Editor

Manuel Pedro Rodríguez Bolívar, University of Granada, Granada, Spain

More information about this series at http://www.springer.com/series/10796

J. Ramon Gil-Garcia • Theresa A. Pardo
Mila Gasco-Hernandez
Editors

Beyond Smart and Connected Governments

Sensors and the Internet of Things in the Public Sector

Springer

Editors
J. Ramon Gil-Garcia
University at Albany
State University of New York
Albany, New York, USA

Universidad de las Americas Puebla
San Andrés Cholula, Puebla, Mexico

Mila Gasco-Hernandez
University at Albany
State University of New York
Albany, New York, USA

Theresa A. Pardo
University at Albany
State University of New York
Albany, New York, USA

ISSN 2512-1812 ISSN 2512-1839 (electronic)
Public Administration and Information Technology
ISBN 978-3-030-37463-1 ISBN 978-3-030-37464-8 (eBook)
https://doi.org/10.1007/978-3-030-37464-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To my Amorecita Nadia, who has shared with me a life full of love and precious moments
—J. Ramon Gil-Garcia

To my dear husband Manuel, with love
—Theresa Pardo

To Marcos, Hawa, and Carlos, the love of my life, and to my Mom and Dad, for being always there
—Mila Gasco-Hernandez

Foreword

During the last decades, information systems became increasingly interconnected. What started with the Internet has evolved into the Internet of Things (IoT), where sensors and actuators are interconnected to measure and control systems from coffee machines to smart cities. This goes along with the collection of more and more data using IoT devices resulting in real-time availability of data about temperature, geolocation, pollution, gas and water flows, force, acceleration, and traffic throughput. These types of data are used already in our daily life. My smart phone warns me if there is a traffic jam, and I have to leave earlier than usual. The daily life of citizens has undergone drastic change and is likely to undergo even more changes (Chatterjee et al. 2018). In a similar vein, government practice is also changing. IoT-generated data provides immense potential for improving our daily life and can be used by the public sector to create societal value. Such types of changes are already visible in evidence-based policy-making in which data collected by IoT is used to develop better policies based on factual data.

The editors of the book recognized the immense opportunity of IoT on our society. J. Ramon Gil-Garcia, Theresa A. Pardo, and Mila Gasco-Hernandez did a wonderful job in bringing together the most recent advances in this field by covering a range of aspects resulting in a multidisciplinary book covering a comprehensive range of topics. They show that IoT is not a standalone technology and needs to be integrated in public administration practice. The adoption and use of IoT is typically an interdisciplinary endeavor in which organization and technical knowledge need to come together.

The relevance of this book does not have to be explained further when looking at the immense possibilities offered by IoT. For instance, IoT is used in smart homes. When my family and I are coming home and it is too cold, my smart home will detect this and will start heating my place. Governments use traffic and pollution data to guide traffic in different ways on a real-time basis and use the same data for the planning of new roads and public infrastructure. IoT can have many benefits ranging from the technical to the strategic level (Brous and Janssen 2015); however, unlocking the value is not easy. The IoT can be used to collect more and more data which can be used by public decision-makers to acquire the necessary insights in a timely fashion. IoT-enabled capabilities in real-time sensing and responding can

spur digital transformation, serve the public interest, and create public value (Chatfield and Reddick forthcoming). To take advantage of IoT as a transformational technology, new organizational and administrative processes are needed, systems need to be adapted, or new systems need to be developed and organizations need to develop new capabilities. IoT can have a transformative effect which requires considerable changes to profit from this technology (Brous et al. forthcoming).

The book consists of two main parts. In the first part entitled "*Theory, Frameworks, and Concepts on Internet of Things (IoT) in the Public Sector,*" the foundations of IoT in government are discussed. A range of issues from participation to security are part of the foundations and should be covered to advance this field. Although many people talk about the IoT, actual use is often limited to smart cities. Collaboration between agencies can be viewed as a condition for success to advance the use of IoT in government (Chatfield and Reddick forthcoming). In the second part of this book entitled "*Applications, Cases, and Experiences of Internet of Things (IoT) in the Public Sector,*" all kinds of international experiences are presented which can be used as a source of inspiration and facilitate learning. There is a need to share practices and conduct comparative research to learn from each other.

Beyond smart government requires the connection of the data generated from IoT with Artificial Intelligence (AI), which in turn can help to intervene in the environment. Algorithms are becoming an integral part of these connected systems like autonomous cars, smart living environments, and smart energy applications for energy transition (Janssen and Kuk 2016). Within these systems, AI can be used for simple tasks like cleaning data to complex decision-making processes involving data from countless distributed sensors. The intelligence provided by systems enable better information sharing and cooperation resulting in improved user-experiences and personalization, higher levels of efficiency, and a reduction of costs. Connected systems integrate data, algorithms, people, processes, and systems to create, for example, connected cars, smart living, and smart energy applications.

IoT is a new topic that has not been discussed widely. In particular in government, this is an area in which research and comprehensive insight is lacking (Brous and Janssen 2015). In this regard, this book fills the void in literature by being the first comprehensive work in the field of IoT in government. This book contributes to unlocking the value of IoT and provides insight to avoid its risks of violating privacy and avoiding security breaches.

Given the increasing use of devices, the knowledge this book provides is a timely and very relevant contribution for organizations wanting to unlock the societal value of IoT and for researchers working in this field. This is an issue that many organizations struggle with and deserves attention. Collaboration is needed, and public organizations need to develop knowledge in this field. This book can help to raise our understanding on how the digital society is shaped.

References

Brous, P., & Janssen, M. (2015). *Advancing e-government using the internet of things: A systematic review of benefits*. Paper presented at the International Conference on Electronic Government.

Brous, P., Janssen, M., & Herder, P. (forthcoming). Internet of Things adoption for reconfiguring decision-making processes in asset management. *Business Process Management Journal*. https://doi.org/10.1108/BPMJ-11-2017-0328

Chatfield, A. T., & Reddick, C. G. (forthcoming). A framework for Internet of Things-enabled smart government: A case of IoT. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2018.09.007

Chatterjee, S., Kar, A. K., & Gupta, M. P. (2018). Success of IoT in smart cities of India: An empirical analysis. *Government Information Quarterly, 35*(3), 349–361. https://doi.org/10.1016/j.giq.2018.05.002

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly, 33*(3), 371–377. http://dx.doi.org/10.1016/j.giq.2016.08.011

Marijn Janssen

Marijn Janssen is full Professor in ICT and Governance and head of the Information and Communications Technology research group of the Technology, Policy and Management Faculty of Delft University of Technology. He worked for the Ministry of Justice and was involved in large transformation projects. He was involved in EU-funded projects in the past (a.o. EGovRTD2020, eGovPoliNet, Engage, VRE4EIC, and OpenGovIntelligence), is co-editor-in-chief of Government Information Quarterly, associate editor of the International Journal of Electronic Business Research (IJEBR), Electronic Journal of e-Government (EJEG), International Journal of E-Government Research (IJEGR), is conference chair of IFIP EGOV-ePart-CeDEM conference series and is chairing mini-tracks at various digital government and information systems conferences. He was ranked as one of the leading e-government researchers in a survey in 2009, 2014, and 2016 and published over 450 refereed publications. He was ranked by Apolitical as one of the 100 most influential people in the Digital Government in 2018 (https://apolitical.co/lists/digital-government-world100). More information: www.tbm.tudelft.nl/marijnj.

Faculty of Technology, Policy and Management,
Delft University of Technology,
Delft, The Netherlands

Acknowledgments

This book is definitively the result of the dedicated effort of many great people who worked together and apart to bring this volume to fruition. We take this opportunity to express our sincere and deep regards and appreciation to all of those who helped and supported us in the conception and completion of this work. A special thank you to all the authors for sharing their knowledge through this editorial project and their interest in the use of sensors and the Internet of Things (IoT) in the Public Sector. This volume would not have been possible without the hard work and collegiality of authors, reviewers, the previous series editor, Christopher Reddick, the new series editor, Manuel Pedro Rodriguez Bolivar, and the staff at Springer. A special thank you to all the reviewers who not only gave their time and effort, but also shared their knowledge through very useful and constructive comments that enhanced the book's overall quality and contribution to the field.

From the staff at Springer, we would like to particularly mention the dedication and commitment of Lorraine Klimowich during the entire editorial process. We always received support and useful guidance from her. We also want to thank Ana Catarrivas, our editorial assistant, whose dedication and diligent efforts have been instrumental for the completion of this book. We are also grateful to CTG UAlbany, formerly the Center for Technology in Government, and the Rockefeller College of Public Affairs and Policy, University at Albany, State University of New York, from which we have received strong institutional support and great encouragement and motivation from colleagues and friends.

Finally, we want to send love and gratitude to our families. They have tirelessly encouraged us and wholeheartedly supported our academic endeavors.

J. Ramon Gil-Garcia
Theresa A. Pardo
Mila Gasco-Hernandez

Contents

About the Editors

J. Ramon Gil-Garcia is an Associate Professor of Public Administration and Policy and the Research Director of the Center for Technology in Government, University at Albany, State University of New York (SUNY). Dr. Gil-Garcia is a member of the Mexican Academy of Sciences and of the Mexican National System of Researchers as Researcher Level III, which is the highest distinction a researcher can obtain before becoming Researcher Emeritus as a result of a lifelong career of research contributions. In 2009, he was considered the most prolific author in the field of digital government research worldwide, and in 2013 he was selected for the Research Award, which is "the highest distinction given annually by the Mexican Academy of Sciences to outstanding young researchers." More recently, Dr. Gil-Garcia was named one of the "World's 100 Most Influential People in Digital Government in 2018" by Apolitical, which is a nonprofit organization based in London in the United Kingdom. Currently, he is also a professor of the Business School at Universidad de las Américas Puebla in Mexico, a Faculty Affiliate at the National Center for Digital Government, University of Massachusetts Amherst, and an Affiliated Faculty member of the Information Science Doctorate Program at the College of Engineering and Applied Sciences, University at Albany. Dr. Gil-Garcia is the author or co-author of articles in prestigious international journals in Public Administration, Information Systems, and Digital Government and some of his publications are among the most cited in the field of digital government research worldwide. His research interests include collaborative electronic government, inter-organizational information integration, smart cities and smart governments, adoption and implementation of emergent technologies, information technologies and organizations, information technologies and education, digital divide policies, new public management, public policy evaluation, and multi-method research approaches. Dr. Gil-Garcia has extensive teaching experience and has collaborated with 11 universities, including departments of Public Administration, Political Science, Social Science, Information Studies, and Management Information Systems. Dr. Gil-Garcia also has many years of experience as a consultant for federal, state, and local government agencies.

Theresa A. Pardo is Director of CTG UAlbany, an applied research institute at the University at Albany, State University of New York, where she is also a full research professor in Rockefeller College of Public Affairs and Policy. CTG UAlbany works closely with multi-sector and multidisciplinary teams from the USA and around the world to carry out applied research and problem-solving projects focused on the intersections of policy, management, and technology in the governmental context. Dr. Pardo serves as OpenNY Adviser to New York State's Governor Andrew Cuomo and is Chair of the U.S. Environmental Protection Agency's National Advisory Committee. She serves as a member of the User Working Group of the NASA Socioeconomic Data and Applications Center (SEDAC), the Business and Operations Advisory Committee of the U.S. National Science Foundation, and the Steering Committee of the U.S. National Science Foundation funded North East Big Data Innovation Hub. Dr. Pardo is founder of the Smart Cities, Smart Government Research-Practice Global Consortium, and a Past-President of the Digital Government Society. In 2018, Dr. Pardo was named as one of the Top 100 Influencers in Digital Government globally. She is also a recipient of *Government Technology Magazine'*s Top 25 Doers, Drivers, and Dreamers Award which recognizes individuals throughout the USA who exemplify transformative use of technology that is improving the way government does business and serves its citizens. Dr. Pardo is a recipient of the University at Albany's Distinguished Alumni Award, the University at Albany's Excellence in Teaching Award, and the Rockefeller College Distinguished Service Award. Dr. Pardo holds a Ph.D. in Information Science from the University at Albany, SUNY.

Mila Gasco-Hernandez holds an MBA and a Ph D in Public Policy Evaluation (Award Enric Prat de la Riba granted to the best Ph D thesis on public management and administration, given by the School of Public Administration of Catalonia in Barcelona, Spain). She is the Associate Research Director of the Center for Technology in Government as well as a Research Associate Professor at the Rockefeller College of Public Affairs and Policy, both at the University at Albany—SUNY. Before joining SUNY, Dr. Gasco-Hernandez served as a senior researcher at the Institute of Governance and Public Management (currently known as ESADEgov—Center for Public Governance) and the Institute of Innovation and Knowledge Management, both at ESADE Business and Law School in Spain. Previous to that, she was a senior analyst at the International Institute on Governance of Catalonia and a professor in Rovira i Virgili University and Pompeu Fabra University, both in Spain.

Mila Gasco-Hernandez has considerable consulting experience on the information and knowledge society as well. In this respect, she has worked for a wide variety of organizations such as the United Nations Development Programme, the Mayor's Office in Valencia (Venezuela), the Spanish Agency for International Development Cooperation, the City Council and the Provincial Council of Barcelona, the International Institute for Democracy and Electoral Assistance, the Latin American Centre on Management for Development (for whom she co-developed the Ibero-American Interoperability Framework), the World

e-Governments Organization of Cities and Local Governments (she was the leading judge for the WeGo Awards), the Inter-American Development Bank, or Google.

Her areas of research are mainly related to information and technology in government and, among others, they include electronic and open government, e-governance, public sector innovation, smart cities, and public policy evaluation.

Chapter Summaries

Chapter 1: The Internet of Things (IoT) is the newest example that fills the gap between cyber world and physical world. The Internet of Things is poised to revolutionize state and local governments. The transformational journey of IoT promises the power to change the world in such a way that people will get closer to their fully integrated and smart surroundings for better management of energy, health, transportation, and life resources. This chapter aims to introduce the presence and relevance of the study of the Internet of Things from a government and public policy perspective.

Chapter 2: The IoT is a revolutionary development for both society and governments. In this chapter, opportunities and threats of the IoT are discussed. Linking technological, societal, economic, and policy-oriented aspects of the IoT, this chapter introduces a conceptual framework to map and analyze the factors or obstacles that arise in addressing IoT opportunities and threats, and possible government measures to mitigate these factors. By adopting a broad view and paying attention to the relations between different factors, this chapter shows that there is no one-size-fits-all solution for IoT-related issues, as different problems and solutions are interdependent and require a coherent government approach.

Chapter 3: Smart cities seek to address public issues via digital connected solutions on the basis of a multi-stakeholder, municipally based partnership. This urban model includes using Internet of Things (IoT) facilities to deliver public services. However, the implementation of public service delivery and use through IoT in smart cities is frequently fragmented, hindering a sustainable urban development. Citizens remain unaware of various single tools developed without their participation. Security issues also prevent citizens from using IoT facilities in smart cities. The objective of this chapter is to explain the development of a participatory governance approach, aiming to establish a sustainable development path for the design and implementation of public services for work and mobility, delivered through IoT in smart cities. Progressing from key issues extracted from existing research about public service delivery using IoT in smart cities, the approach adopts a socio-technical, processual methodology combining several social research methods as well

as visualization and game simulation techniques. The chapter concludes with a short discussion about the application of this participatory framework in the ongoing design and evaluation of sustainable public service delivery using IoT in smart cities.

Chapter 4: This chapter reviews the expanding role of the Internet of Things (IoT) in our lives as well as the security concerns of IoT. While IoT has expanded enormously in recent years both in the private and public sectors where it has enhanced the quality of life, it has also created potential security risks for users in various ways, such as in enabling unauthorized access and misuse of personal information, facilitating attacks on other systems, and creating safety risks. Even though these risks were already common in cyberspace contexts, the introduction of IoT has increased these risks given its role in expanding the Internet and its connections to every aspect of our daily lives. This chapter will provide a systematic review of the current literature of IoT in order to identify IoT security challenges, and to offer recommendations for responding to these challenges. As a result of our study, we identified pervasiveness, privacy, and vulnerability as main challenges that are discussed in the literature. In this research, we also compiled some recommendations such as encryption, cryptology, authentication, authorization, and advanced security frameworks, schemes, and protocols to respond current security challenges in the IoT. Policy recommendations are also discussed to give ideas to policymakers about IoT security.

Chapter 5: Blockchain technology is attracting the interest of professionals and academics across a variety of disciplines, including the interdisciplinary field of Digital Government. Such technology has the potential to transform the public sector by providing innovative ways to secure data and avoid tampering. However, few studies have theorized on experimental applications of such technology and how it could be applied to data management practices in data-rich environments such as the Internet of Things (IoT) applications in smart cities. This chapter proposes a workflow diagram for technical experiments that explore how blockchain technology can protect the integrity of data from sensors in a context where IoT is the underpinning infrastructure. This endeavor helps to contextualize this emerging technology and sheds light on opportunities, risks, and challenges of using blockchain technology in environments where intensive data collection is the norm. Contributions include a framework on data management for IoT that can be of special value to local governments that are considering blockchain as instrumental in engaging in or enhancing data-driven operations.

Chapter 6: This chapter explores implementation challenges as opportunities for moving beyond smart and connected governments by focusing on awareness in relation to sensing, sensors, and the Internet of Things (IoT) in the public sector in the context of smart cities. A review of the research literature for smart city implementations is conducted from multiple perspectives highlighting a range of issues and challenges for the public sector. The theoretical framework for this chapter uses the construct of awareness in relation to the key smart city characteristics of adaptability,

complexity, innovation, and readiness. The research design for this work utilizes a single case study approach to explore evolving understandings of smart city implementations in contemporary urban environments. Multiple methods of data collection are used including survey and interview while content analysis is used in the iterative analysis of data. Data were collected and analyzed from diverse individuals in multiple small- to medium- to large-sized cities, mostly in Canada and extending to other countries (e.g., Israel). This work makes several contributions by providing: (a) an expanded way of looking at IT implementation in the public sector for twenty-first century urban environments encompassing sensing, sensors, and the IoT; (b) understandings of IT implementation challenges as opportunities in the public sector for more responsive and aware solution-making; and (c) a conceptual framework for more dynamic notions of implementation in the public sector, as in, ambient implementation. This chapter advances an awareness-based explanatory model for ambient implementation of use to the public sector in smart cities.

Chapter 7: The Internet of Things is being actively introduced in Russian public governance for inspection and oversight. In this chapter, based an analysis of IoT policy, legal acts, secondary statistical data, and the authors' own involvement in testing IoT technologies, we formulate cases and use them as a basis for an IoT classification oriented to the needs of government agencies. The spheres of application we consider are transport, justice, retail, and manufacturing. The case we study in greatest detail is that of the fur industry. We apply the method of cost-benefit analysis and examine the costs of using IoT in public governance to regulate the turnover of fur goods as well as the benefits for key stakeholders (government, society, business). We identify barriers that prevent IoT technology from being used effectively and describe the effects of implementing IoT in the fur industry and other areas in which IoT is used for inspection and oversight.

Chapter 8: Since 2014, the question of the implementation of the Internet of Things has been crucial in France. Public authorities have created arenas where digital entrepreneurs and politicians can discuss the evolution of the Internet of Things. In January 2017, the National Assembly published a report on the economic and social consequences of the adaptation of the Internet of Things. This chapter analyzes the political discourse that gives legitimacy to the implementation of the Internet of Things in France. The digital entrepreneurs are the privileged actors of this implementation, their social recognition by the French Parliament and the labeling campaigns (French Tech) reinforce the myth of technological innovation. The field of the critical analysis of discourse is mobilized to evaluate the spread of this new myth in France and the analysis of the legitimization of the digital entrepreneurs. This case study reveals how European countries tackle new digital policies in order to control the evolution of the Internet of Things and the field of Artificial Intelligence.

Chapter 9: In its simplest form, smart government can be understood as the combination of new technologies and organizational innovation strategies to further modernize the public sector. Within this development, the Internet of Things (IoT) often forms a key technological foundation, offering government authorities new

possibilities for interaction with citizens and local communities. On one hand, citizens can indirectly participate in governmental services' value creation by using public infrastructure or (un)knowingly sharing their data with the community. On the other hand, smart government initiatives may rely more intensively on citizens' active participation to improve public service delivery, increase trust in government actions, and strengthen community sentiment. In this chapter, we discuss active and passive participation scenarios of smart government initiatives and explain how sensor-based systems may enhance citizens' opportunities to participate in local governance. We present two practical cases from Switzerland demonstrating these two citizen involvement modes. We argue that active and passive participation of citizens and other stakeholders play key role in generating necessary data for algorithmic decision-making to enable personalized interaction and real-time control of infrastructure in the future. We close with a discussion of the possibilities and boundaries of the IoT in the public sector and their possible influences on citizens' private lives and policy-making.

Part I
Theory, Frameworks, and Concepts on Internet of Things (IoT) in the Public Sector

Internet of Things and the Public Sector

J. Ramon Gil-Garcia, Theresa A. Pardo, and Mila Gasco-Hernandez

Abstract The Internet of Things (IoT) is one of the most recent examples of a technology that has the potential to bridge the cyber world and the physical world. The IoT can be understood as the integration of a great number of small devices (including many types of sensors, which are components capable of detecting changes in its environment and converting this change into an electrical signal) into a network that shares and integrates their data, which can be used for real-time decision-making. The transformational power of the IoT promises to change the world by fully integrating people into their surroundings for better management of energy, health, transportation, and life resources. In the public sector, the IoT has the potential to revolutionize federal, state, and local government programs and services, particularly in domains in which the physical infrastructure or the natural world are key elements of those programs. This chapter conceptualizes the IoT, outlines some potential benefits generally and in the public sector, and presents some of the challenges to adoption and use of the IoT. The chapter closes with an overview of the subsequent book chapters.

Keywords Internet of things · IoT · Public sector · Public policy · Government · Sensors

J. R. Gil-Garcia (✉)
University at Albany, State University of New York, Albany, New York, USA

Universidad de las Americas Puebla, San Andrés Cholula, Puebla, Mexico
e-mail: jgil-garcia@ctg.albany.edu

T. A. Pardo · M. Gasco-Hernandez
University at Albany, State University of New York, Albany, New York, USA
e-mail: tpardo@ctg.albany.edu; mgasco@ctg.albany.edu

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_1

Introduction

The Internet of Things (IoT) is one of the most recent examples of a technology that has the potential to bridge the cyber world and the physical world. The IoT could be understood as the integration of a great number of small devices (including many types of sensors, which are components capable of detecting changes in their environment and converting those changes into an electrical signal) into a network that shares and integrates their data, which can be used for real-time decision-making. Since fiscal year 2011, federal government spending on the IoT has grown at a compound annual rate of 10 percent (Perera et al. 2014). Growth figures such as those presented during the OECD's 2014 Technology Foresight Forum provide further evidence of interest in the IoT: "The number of connected devices in households in OECD countries is expected to be 14 billion by 2022, up from around 1.4 billion in 2012, or to put it differently, from 10 connected devices in a household with two teenagers to 50 in ten years' time" (OECD, Technology Foresight Forum, 2014). It is estimated that by 2020, there will be 50–100 billion devices connected to the Internet (Sedrati and Mezrioui 2018). The vision of the IoT is to allow "things" to be connected anytime, anyplace, with anything and anyone (Perera et al. 2014). In general terms, the IoT refers to a network of interconnected everyday objects. It comprises billions of connected "things" or devices that can sense, communicate, compute, and potentially actuate. These objects have intelligence, multimodal interfaces, and physical/virtual identities and attributes (Perera et al. 2014).

Maximizing the potential of the IoT requires understanding of the technology itself, as well as a consideration of that technology within potential use contexts (Werthmuller 2016). Understanding the nature of the IoT and its potential to create value across the sectors is still in its nascent stages. However, in recent years, the IOT has gained much attention from researchers and practitioners from around the world (Xia et al. 2012). For instance, Erfanmanesh and Abrizah (2018) found that there has been a continuous increase in the number of scholarly publications about the IoT per year over the period between 2011 and 2016, with a 6.7-fold rise in the number of publications and the highest share of research output (4989) published in 2016. Research on the IoT has largely focused around single application domains or single technologies (Miorandi et al. 2012).

This book makes a unique contribution to efforts to understand the IoT and its value-creation potential in the public sector, specifically through an integrative examination of the relevant literature and presentation of a set of studies that introduce concepts and frameworks for IoT use, present methodologies for building understanding of the IOT, and provide case studies.

This chapter introduces the concept of the IoT by highlighting definitional elements from the literature, implications for use, and potential applications in the public sector context. The chapter is organized in seven sections, including the foregoing introduction. Section "Conceptualizing the Internet of Things (IoT)" presents some definitions of the IoT from the academic literature. Section "Potential Benefits of IoT" includes some of the potential benefits of the Internet of Things. Section "IoT and the Public Sector" describes and explains how the IoT could affect the

public sector. Section "Challenges to Creating Value with the IoT" discuss some of the expected challenges to the use of Internet of Things. Section "A Book on the IoT from a Public Sector Perspective" presents brief summaries of the chapters included in this book and section "Concluding Remarks" offers some final comments and ideas for future research about this topic.

Conceptualizing the Internet of Things (IoT)

The phrase "the Internet of Things" is syntactically composed of two terms. The first one pushes towards a network-oriented vision, while the second one moves the focus onto generic "objects" to be integrated into a common framework (Atzori et al. 2010). Semantically speaking, the "Internet of Things" means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" (Infso 2008), which implies a huge number of (heterogeneous) objects involved in the process. At its inception, the concept was related to the use of emerging sensor technologies and radio frequency identification (Sundmaeker et al. 2010).

The term "the Internet of Things (IoT)" seems to act as an umbrella concept that covers various features such as the extension of the Internet, the web as a physical realm, deployment of extensive embedded distributed devices, and actuation abilities (Miorandi et al. 2012). Some call it the "Internet of everything," defined as "people, process, data and things to make networked connections more relevant and valuable than ever before, turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries" (Hatem et al. 2016).

Today, many mobile devices have built-in sensors (e.g., a GPS sensor or an accelerometer). These sensors can be useful for tasks such as traffic monitoring. The data collected can be analyzed using a range of techniques, and used for predictions, pattern recognition, forecasting, visualizations, and decision support (Johannessen and Berntzen 2016).

In the vision of the IoT, an increasing number of embedded devices of all sorts are capable of communicating and sharing data over the Internet (Zeng et al. 2011). The IoT will increase the ubiquity of the Internet by integrating every object for interaction via embedded systems, leading to a highly distributed network of devices communicating with human beings as well as other devices. The condition required to make something an IoT object is that it contains a sensor/actuator that can communicate and support the three pillars of the interconnection of smart objects: identification, communication, and interaction (Sedrati and Mezrioui 2018; Bilal 2017).

From a research perspective it is more difficult to understand what exactly the IoT is and what the technical, economic, and social implications of full deployment of the IoT may be (Atzori et al. 2010). For some authors, the IoT represents the next evolution of the Internet; it is increasing the universality of the Internet by integrating every object for interaction via embedded systems, creating a highly distributed

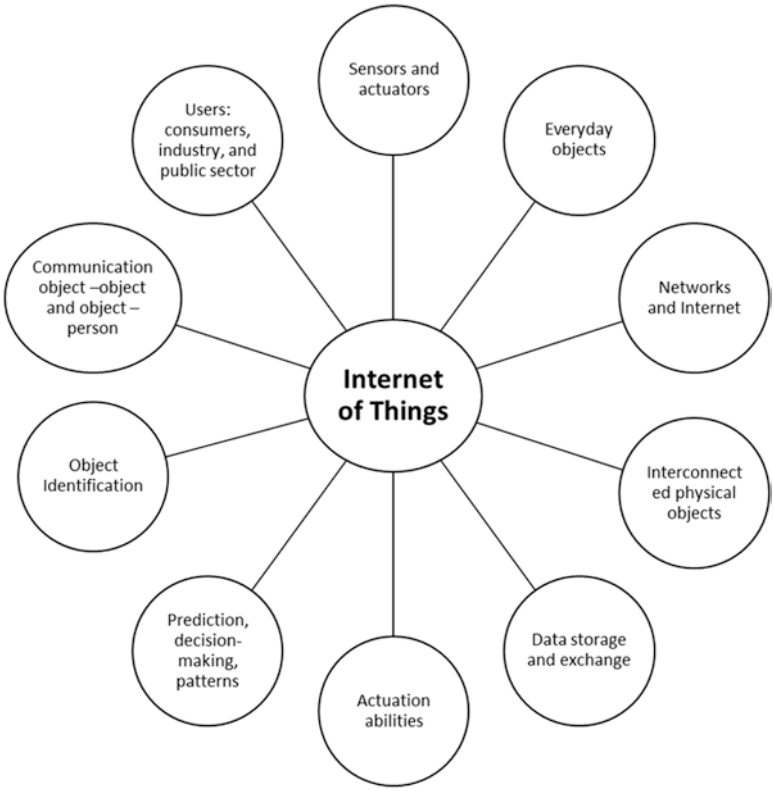


Fig. 1 Some elements of definitions of the IoT

network of devices communicating with human beings as well as other devices. Figure 1 presents some of the most commonly mentioned elements from definitions of the IoT found in the literature.

Several definitions from the field of computer science describe the IoT as a network of physical devices having sensing and network capabilities that enable the devices to store and exchange data. Such a network is considered to be a bridge between various technologies (Middha and Verma 2018). Chui et al. (2010) define the IoT as sensors and actuators embedded in physical objects—from roadways to pacemakers—linked through wired and wireless networks, often communicating with the same Internet Protocol as the Internet. Latif et al. (2018) define the IoT as a network of miscellaneous items such as physical devices, automobiles, and home appliances, embedded with sensing, networking, and communication technologies in order to connect and communicate. The main components of the IoT are objects that communicate with each other, the Internet as the communication medium, hardware that collects data from objects, and platforms that enable communication and decision-making (Keskin and Kennedy 2015).

As a new technology allowing many "things" to be connected for the first time ever, the IoT marks a clear difference with the classical Internet where only given devices could do so (Sedrati and Mezrioui 2018). The technology implies a high level of complexity, when you transition from an Internet used for interconnecting end-user devices to an Internet used for interconnecting physical objects that communicate with each other and/or with humans. The IoT can provide communication, connection, and inter-networking between various devices or physical objects. However, most of the things in the IoT have limited power, storage (Middha and Verma 2018), and computational capabilities. Therefore, data are collected, manipulated, and stored in the cloud (Sen et al. 2018), raising questions about information management (Gohar et al. 2018) and processing (Perera et al. 2014).

Din et al. (2017) see the IoT as a powerful technology that helps in understanding the physical world and enables response to stimuli. The things in the IoT can sense the physical environment, collect data, transfer or disseminate data, process data for appropriate applications, and communicate with other things, with no human intervention in most cases, yet also serve as a source of information for a human being (Sivakumar et al. 2017). Due to the advances in sensor and cloud technology, processing and storage capability, and decreased sensor production cost, the growth of sensor deployments has significantly increased over recent years (Perera et al. 2014). Examples include street lights being networked and things like embedded sensors, image recognition functionality, augmented reality, and near field communication integrated into situational decision support, asset management, and new services (Atzori et al. 2012; Sivakumar et al. 2017).

Although there is no generally accepted definition of the IoT (Whitmore et al. 2015), existing definitions seem to agree on several aspects of the IoT: (1) it contains ubiquitous "everyday" objects (i.e., mobile phones, smoke detectors, cars, wearables, home appliances) that are accessible through the Internet and equipped with sensing, storing, and processing capabilities that allow these objects to understand their environments; (2) it contains identifying and networking capabilities that allow them to communicate information about themselves; (3) it involves object–object, object–person, and person–person communication; and (4) it can make autonomous decisions. If they fulfill those pillars, things can be considered to be "smart objects" (Sedrati and Mezrioui 2018).[1]

Potential Benefits of IoT

Thanks to rapid advances in underlying technologies, the IoT is creating tremendous opportunities for novel applications across domains and sectors that promise to improve the quality of life (Xia et al. 2012; Sedrati and Mezrioui 2018). In the

[1] Readers may find several more categorizations in the literature, the ones presented here are for descriptive purposes only and this is not a definitive list.

view of Keskin and Kennedy (2015), machines that we interact with in everyday life will start interacting with each other, collecting data, and using advances in data technologies to make decisions for us. Today, consumers can use the IoT devices to collect personal information for tasks like monitoring health and automating household functions. Industry is already benefitting from the IoT through optimizing processes and related cost savings. Going forward, sensors that have always been an integral part of factory setup for security, automation, and climate control, among other uses will eventually be replaced by wireless systems, thereby optimizing processes, generating cost savings, and providing capability to make changes to the setup whenever required (Lakshmi 2018).

From the point of view of an individual, the most obvious effects of the IoT introduction will be at home and at work. In this context, *domotics* (the use of information technology for home automation), assisted living, e-health, and enhanced learning are only a few examples of possible application scenarios for the new paradigm. Similarly, from the perspective of business users, the consequences of the IOT will be visible in fields such as automation and industrial manufacturing, logistics, business and process management, and intelligent transportation of people and goods (Atzori et al. 2010). The IoT has significant potential in high-risk Environment, Health, and Safety (EHS) industries. In these industries, human lives are at stake and the IoT-based applications are primed to offer safe, reliable, and efficient solutions due to their ability to operate at a fine granular level and provide rich low-level information (Thibaud et al. 2018).

Smart Cities, Smart Homes, Smart Healthcare, and many more innovative applications have been implemented in countries such as Japan, Korea, Canada, and Russia (Sivakumar et al. 2017). Public sector organizations and communities are using the IoT devices to address concerns related to the existing physical infrastructure or the natural environment. Figure 2 shows some potential benefits of the IoT. New applications for the IoT will be designed to improve the quality of our lives in the home, while travelling, when sick, at work, and when exercising. Such applications can be grouped into the following domains: (1) transportation and logistics domain; (2) healthcare domain; (3) smart environment (home, office, plant) domain; and (4) personal and social domain (Atzori et al. 2010).

Many public services are expected to improve with the use of the IoT including traffic management; public safety; water resources management, including quality and usage monitoring; waste management; heating, ventilation and air conditioning (HVAC) management; and environmental air pollution monitoring, among others. Through these improvements, the IoT may have the potential, according to Fosso Wamba et al. (2015), to "revolutionize" public management.

Among the possible applications of the IOT, Atzori et al. (2010) distinguish between those either directly applicable or closer to our current living habits and those that are futuristic, which we can only imagine at the moment, since the technologies and/or our societies are not ready for their deployment (see Table 1) (Atzori et al. 2010).

Within many domains, the IoT is being referred to as a "smart system." Some authors (Middha and Verma 2018) refer to Smart Environment, where everything

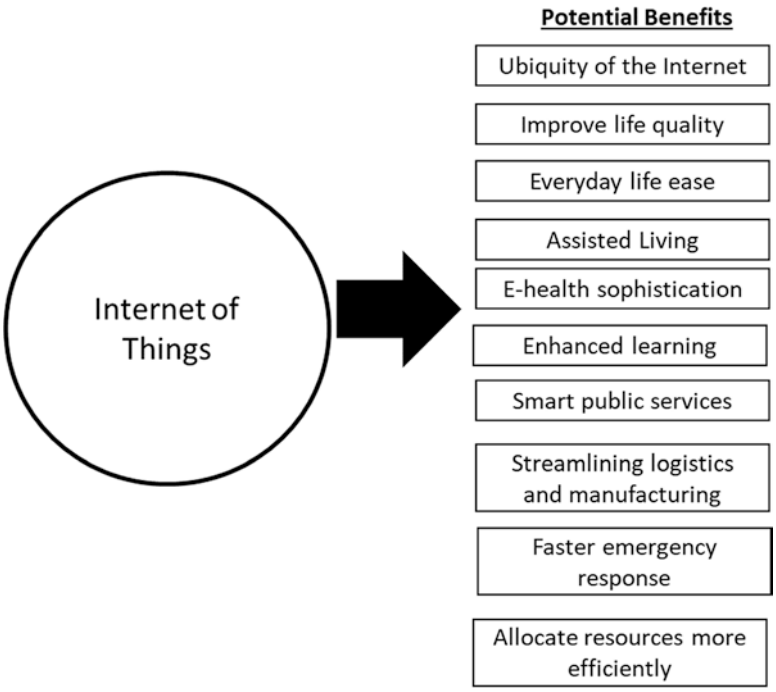


Fig. 2 Some potential benefits of the IoT

Table 1 Examples of IoT applications

Transportation and logistics	Healthcare	Smart environments	Personal and social	Futuristic
Logistics	Tracking	Comfortable homes/offices	Social networking	Self-driving taxi
Assisted driving	Identification, authentication	Industrial plants	Historical queries	City information model
Mobile ticketing	Data collection	Smart museums and gyms	Losses	Enhanced game room
Environment monitoring	Sensing	Retail	Thefts	
Augmented maps		Surveillance	Home utilities and appliances	
Emergency services		Smart metering		
Traffic and highways				

Based on Atzori et al. (2010), with additional examples from Lakshmi (2018), Miorandi et al. (2012), and Whitmore et al. (2015)

comprises a "smart system" such as smart government, smart utilities, and smart buildings (Rajguru et al. 2015). Several research studies agree that the IoT can create value to users by offering solutions that not only save time and money, but also save lives and help organizations, including governments, allocate resources more efficiently (Lee et al. 2017; Lee 2019; Middleton et al. 2013; Wakefield 2014). Many connected devices and services have already begun to reshape homes, factories, cities, vehicles, and hospitals. For example, smart home systems controlled by smart speakers or hubs are changing the way we use and manage home appliances (Lee 2019). While consumer-facing IoT is what most people think of first, the industrial IoT is expected to account for the bulk of GDP growth where gains will be derived from greater efficiencies in asset utilization, employee productivity, supply chain and logistics, customer experience, and innovation (Cho 2015).

IoT and the Public Sector

Government decision makers are beginning to understand the potential of the IoT to create value for citizens. They see the IoT as the network through which information resources may be shared between smart objects (Kortuem et al. 2010) and ultimately used by public entities to enhance the efficiency and effectiveness of government services (Keskin and Kennedy 2015). These decision makers, and others like them, are recognizing the potential of the IoT to transform government programs and services including healthcare, personnel monitoring, disease spread modeling and containment, resource management and distribution, first response planning and implementation, and efficient use of public spaces, among others (Lakshmi 2018). However, they are also recognizing that they need to create a new understanding of where and how the IoT fits into their future plans and needs.

A 2016 survey of 125 US state and local government decision makers conducted by the Center for Digital Government (CDG) shows that governments are investing in evaluations of their current needs and future plans with a particular eye on the IoT. The CDG report indicates that 52 percent of respondents are evaluating their network needs and future plans, and half of them say this activity is triggered by new technologies like the IoT (CDG 2017). They, like decision makers in other domains, are looking to determine which applications of the IoT represent the greatest return on investment. Table 2 presents some examples of the use of the IoT in the public sector. The sections below highlight applications in e-health, education, intelligent transportation, and cities and local governments that are or are expected to create value to citizens.

The IoT is expected to play a key role in connecting the e-health system with the cyber world through new services and seamless interconnection between heterogeneous devices (Din et al. 2017). Research on the IoT in healthcare shows its potential to improve the quality of healthcare (Pal et al. 2018) by enabling preventive care and promoting automation to reduce the risk of human error (Kadarina and Priambodo 2017). Healthcare IoT is expected to boost patient satisfaction by

Table 2 The IoT in the public sector

Services	Response	Cost efficiency	Proximity to citizen
Safety and traffic management	Awareness and response for flooding conditions	Solar powered trash compactors	Interaction between citizens and public agencies evolve
Water quality, usage and distribution	Built in sensors for emergencies	Personnel monitoring	Direct and timely communication
Better time estimates for public transportation	Air pollution monitoring and response	Use of public spaces	
Public health	Data collection for better decision-making	Waste management	
Integrated services of education technology		Electric grid management	

improving efficiency of services, allowing patients to spend more time with their doctors (Sivakumar et al. 2017). Healthcare provision for the elderly using the IoT is expected to increase efficiency and effectiveness of those services (Lin et al. 2017). Boston Medical Center (BMC), for example, has had success using the IoT for patient care and building operations. While many IoT deployments focus on routine operations such as light and heat control, BMC is using the IoT to monitor everything from leftover food to newborn babies (Sivakumar et al. 2017).

The education sector is likely to become heavily impacted as schools and universities make greater use of connected devices. For example, Quick Response (QR) codes have made their way into educational textbooks. Feedback, assignments, and additional knowledge resources become easily available to students when they scan the QR codes with their smartphones. Another example is the radio frequency identification (RFID) chips that are being used by students to tag and track physical objects to study them. In addition, IoT devices are being used by university administrators and instructors to take automatic attendance using student ID cards, track equipment, and monitor lighting and security systems (Mershad and Wakim 2018). According to Lopez (2013), the IoT in education creates a new environment that supports the acquisition of knowledge in a new and efficient manner that is consistent with the learners' needs and expectations.

The IoT allows public asset managers to access remote sensor data and to monitor and control the physical world from a distance, allowing many physical objects to act "in unison" (Ramos et al. 2018). Because of its ubiquitous sensors and connected systems, the IoT can provide authorities with more information and control in order to identify and fix problems with critical infrastructure. Efficient energy consumption, for example, can be achieved by continuously monitoring every electricity point within a building and using this information to modify the way electricity is consumed. At scale, this technology can be used for maintaining load balance across an entire grid, ensuring high quality of service (Lakshmi 2018).

Intelligent transportation through real-time traffic information and path optimization has the potential to create value for citizens. The IoT can be used to collect data to determine the position and length of traffic jams, and to redirect traffic or offer alternative multimodal forms of transport by using location sensors and analyzing traffic flow (Brous et al. 2018). Traffic data over a period of time in a specific place can help decision makers to make long-term strategic choices, such as whether to invest in a tram service across the city or not.

Further, the IoT is also expected to have a large impact on public transportation, where GPS tracking devices allow real-time monitoring of buses and trains to provide better wait time estimates (Sivakumar et al. 2017). Train collision avoidance systems (TCAS) provide another interesting example of the use of the IoT in transportation management. In TCAS implementations, a sensor is placed beneath the track, which senses the pressure, temperature, and altitude of the track. The system then uses the data from the sensor to prevent train collisions by allowing authorities to take action before collision or derailment of trains takes place, therefore saving lives (Savner and Gugapriya 2018).

Cities and other local government are benefiting from the IoT in a variety of ways. For many cities, becoming a "smart city" includes the use of IoT solutions to manage city assets. Managing city assets or systems, through the use of the IoT is leading to improvements in traffic control, education, transportation, building and bridge monitoring, emergency response coordination, and hospitals, among other systems (Gascó 2017; Gil-Garcia et al. 2013; Middha and Verma 2018; Lakshmi 2018). The IoT is already enabling smart city deployments for technologies like connected streetlights and meters and the use of new data in decision-making (Brous et al. 2018). Some examples of IoT implementation in cities and other local governments in the USA include the following: (1) Los Angeles connected 145,000 streetlights and 4500 intersections to the Internet to improve safety and traffic management; (2) the Lower Colorado River Authority in Texas Is exploring sensors for river levels that will improve awareness and response for flooding conditions; (3) Miami-Dade County in Florida installed controllers on traffic signals to support future connections with smart cars, public transit, and other vehicles; and (4) Chicago and Philadelphia use solar-powered trash compactors that automatically send alerts when they need to be emptied (Harbert 2017).

While the IoT is being used in many different ways, the uses appear to be directed at a set of common goals including (1) connected physical safety and security, (2) saving money by increasing efficiency and employee productivity, (3) automating decision processes rather than providing information that humans can use to make decisions, and (4) applying the IoT to long-standing practices to achieve additional benefits. The use of the IoT and the data produced through it will have an impact on individual government agencies and government operations as a whole, potentially changing the very nature of the relationships between government, citizens, and other stakeholders. They present opportunity, but also critical challenges to governments in both the developed and developing world and across levels and branches of government. The next section introduces some of these challenges.

Challenges to Creating Value with the IoT

As a technology combining real-life objects and virtual life (Internet), the IoT is a fertile ground for innovation and new ideas. However, ensuring that implementations of the IoT deliver the expected benefits is challenging (Sedrati and Mezrioui 2018; Jesus et al. 2018). As Lee (2019) points out, while the potential of the IoT to contribute to economic growth and social welfare is indisputable; its success is not guaranteed without thoughtful strategies to drive a "pro-innovation environment." Some domains and sectors, such as the public sector, will face additional challenges related to those contexts. Even though smart sensors and IoT technologies have great potential to transform public service provision, the adoption and use of the IoT in the public sector, not unlike other such transformative technologies, is proving to be slow and incremental (Tang and Ho 2018). It is not surprising then, that according to Jesus et al. (2018), the rapid emergence of the IoT is complicating life for state and local IT departments.

Unfortunately, due to the nascent stage of the IoT and the lack of a robust literature on the IoT, and in particular, very few empirical studies on its adoption and use, we are just beginning to understand the challenges to creating value with the IoT. Insights are beginning to coalesce from studies such as the one conducted in 2013 by the Economist Intelligence Unit (CDG 2017) which recognize the challenges to the IoT as (1) a lack of employee skills and expertise; (2) a lack of knowledge or commitment shown by management; (3) no explicit IoT element in the products; (4) the immaturity of industrial standards; and (5) the high costs of building an IoT infrastructure. Harbert (2017) points to a lack of strategic leadership on how to use the IoT; a lack of skills in using the data generated by the IoT; insufficient funding to modernize IT infrastructure to enable IoT projects; procurement policies that make it difficult for governments to quickly and easily adopt the technology; and risk and uncertainty about privacy, security, interoperability, and return on investment as additional challenges.

Brous and Janssen (2015) speak to the IOT's impact on organizational structures and cultures related to the automating of processes. Challenges are arising as tasks previously performed by people become automated, while other tasks and responsibilities which previously did not exist become relevant. Jaafreh (2018) identifies challenges related to cultural beliefs and technology acceptance. Work by Raffman and Russo (2018) calls attention to the product liability and regulatory risks arising from the potential for digital failures to cause serious physical-world impacts, including property damage and personal injury. Figure 3 shows some of the main challenges to the IoT as found in the literature.

Some of the identified challenges can be described quite easily, such as the fact that IoT objects need to have sensors and actuators connected and ready presenting a clear challenge in terms of energy (Middha and Verma 2018). How will sensors be charged? Other challenges are quite complex, such as security and outdated regulations and governance. None of the challenges, whether simple or complex, are easy

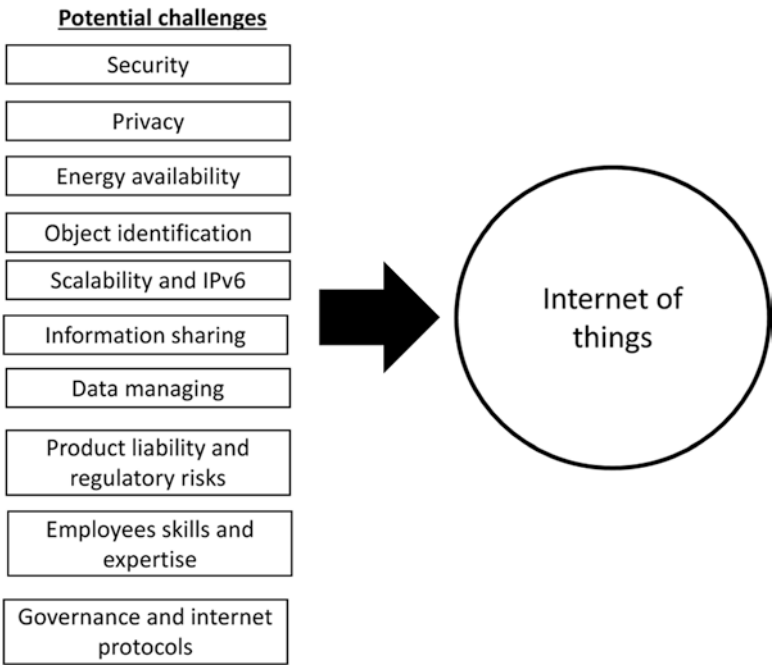


Fig. 3 Potential challenges to the adoption and use of the IoT

to overcome. A few of the more well-studied challenges are discussed in more detail below.

Security concerns seem to be one of the main reasons for slowing IoT implementations in government. The benefit of "anytime and anywhere" access to data has given rise to serious security and privacy issues and is leading to problems such as exposure of a user's personal and sensitive information and loss of the trust between parties (Liu et al. 2018; Middha and Verma 2018; Perez et al. 2018; Sen et al. 2018). With millions of devices, sensors, buildings, vehicles, and other things connected to the Internet (often wirelessly), state and local governments, among others, are working to figure out how to secure this new digital connective tissue and the data that flow through it. Lack of awareness and inconsistent security across all endpoints leave organizations vulnerable to attack. To have functional and secure IoT technology in the future, issues such as sensors/actuators and privacy need to be investigated and solved (Sedrati and Mezrioui 2018).

The identification of the objects is another important challenge. Should each object have a unique identification or a group, some type of "label"? This matter is linked to questions regarding property and ownership (Alshehri et al. 2018). Should all objects be treated equally and have the same technology and network or should there be groups (aircrafts, buildings, cars, domestic appliances, and so forth)? It is not clear if all the devices will use the same set of protocols and data formats, due to their different processing and storage capabilities and size. Further, the world ran

out of IPv4 addresses in February 2010. While no real impact has been seen by the general public, this situation has the potential to slow the progress of the IoT since the potentially billions of new sensors will require unique IP addresses. It is still unclear if IPv6 will solve this problem, and if so, when.

The lack of adequate and updated regulation and governance protocols is also a significant challenge. As the number of connected things increases, so too does the need for governance. A 2017 CDG survey identified outdated policies as the top concern of all respondents. A strong governance structure for IoT-related decision-making in the public sector is recognized as critical and missing. The questions of who decides and how they decide it are not new; the same issues plague the governance of Internet protocols as well. For example, the IoT systems development stack is still evolving at a rapid pace and currently without any prominent and widely agreed-upon architectures or technology solutions. In fact, non-interoperability of the heterogeneous technologies currently used in city and urban developments has been found to be one of the leading challenges in developing IoT applications in public services (El-Haddadeh et al. 2018; Zanella et al. 2014).

An overarching challenge, regardless of sector, is scalability. Regardless of the specific challenge to the IoT being considered, the solution strategies being considered to mitigate that challenge must be scalable. The IoT is expected to have more objects and more types of things connected in the near future, yet today there is no research focused on ensuring that the developed IoT solutions are scalable across billions of IoT nodes (Alshehri et al. 2018). Scalability has to address interconnection, information sharing and use, and knowledge management challenges as well. From a scalability perspective, the large number of IoT devices increases the risk of security threats such as viruses or cyberattacks (Alshehri et al. 2018).

When situated in the public sector, each of these challenges takes on a unique character. Information confidentiality becomes more delicate. Heterogeneity among local, state, and federal efforts can be overwhelming. Scalability in order to reach more citizens and more areas of government is necessary, yet introduces new complexities and vulnerabilities, as well as creating greater resource requirements. One of the leading challenges in developing IoT applications in public services is the non-interoperability of the heterogeneous technologies currently used in city and urban developments (El-Haddadeh et al. 2018; Zanella et al. 2014).

A Book on the IoT from a Public Sector Perspective

This book provides one of the first comprehensive approaches to the study of sensors and the IoT from a government and public policy perspective. The book includes concepts and frameworks for understanding opportunities and challenges governments face when seeking to improve public services and government operations through the use of the IoT. It includes innovative methodologies for building an understanding of the potential of a smart and connected government. In addition, the book offers relevant and recent case studies and practical recommendations. The

chapters address diverse technologies, applied to several contexts, as well as different levels and branches of government. As a whole, the book argues that sensors and the IoT can enhance the public sector's ability to create public value and will present critical challenges that need to be understood and managed if the potential of the IoT is to be realized by the world's governments. In that sense, the target audience will be academics and professionals who want to improve their understanding of sensors and the IoT at all levels and branches of government and in very different political, economic, and cultural contexts.

In the chapter "The Internet of Things in a Smart Society: How Government Policy Can Help Seize Opportunities and Mitigate Threats", Ronald Pool, Jasper van Berkel, Susan van den Braak, Maaike Harbers, and Mortaza Bargh explain how the IoT is a revolutionary development for both society and governments. In this chapter, the authors discuss opportunities and threats of the IoT. Linking technological, societal, economic, and policy-oriented aspects of the IoT, this chapter introduces a conceptual framework to map and analyze the factors or obstacles that arise in addressing IoT opportunities and threats, and possible government measures to mitigate these factors. By adopting a broad view and paying attention to the relationships between different factors, this chapter shows that there is no one-size-fits-all solution for IoT-related issues, as different problems and solutions are interdependent and require a coherent government approach.

In the chapter "Methodologies for a participatory design of IoT to deliver sustainable public services in 'smart cities'", Esther Ruiz Ben focuses on how smart cities seek to address public issues via digital connected solutions on the basis of a multi-stakeholder, municipally based partnership. This urban model includes using IoT facilities to deliver public services. However, the implementation of public service delivery and use through the IoT in smart cities is frequently fragmented, hindering sustainable urban development. Citizens remain unaware of various single tools developed without their participation. Security issues also prevent citizens from using IoT facilities in smart cities. The objective of this chapter is to explain the development of a participatory governance approach, aiming to establish a sustainable development path for the design and implementation of public services for work and mobility delivered through IoT in smart cities.

Authors Guler and Demir reviewed the expanding role of the IoT in our lives as well as the security of the IoT. Their chapter (Identifying Security Challenges in the IoT for the Public Sector: A Systematic Review) argues that while the IoT has expanded enormously in recent years both in the private and public sectors to enhance the quality of life, it has created potential security risks for users in various ways, such as in enabling unauthorized access and misuse of personal information, facilitating attacks on other systems, and creating safety risks. Even though these risks were already common in cyberspace contexts, the introduction of the IoT has increased these risks given its role in expanding the Internet and its connections to every aspect of our daily lives. This chapter provides a systematic review of the current literature of the IoT in order to identify IoT security-related challenges, and to offer recommendations for responding to these challenges. As a result, the authors

identified pervasiveness, privacy, and vulnerability as main challenges that are discussed in the literature.

Blockchain technology is attracting the interest of professionals and academics across a variety of disciplines, including the interdisciplinary field of Digital Government. In the chapter "Using Blockchain Technology to Manage IoT Data for Smart City Initiatives: A Conceptual Framework and Initial Experiments based on Smart Contracts", Fan, Cronemberger, and Gil-Garcia explain how such technology has the potential to transform the public sector by providing innovative ways to secure data and avoid tampering. However, few studies have theorized experimental applications of such technology and how it could be applied to data management practices in data-rich environments such as the IoT in smart cities. This chapter proposes a workflow diagram for technical experiments that explore how blockchain technology can protect the integrity of data from sensors in a context where IoT is the underpinning infrastructure. This endeavor helps to contextualize this emerging technology and sheds light on opportunities, risks, and challenges of using blockchain technology in environments where intensive data collection is the norm. Contributions include a framework on data management for the IoT that can be of particular value to local governments that are considering blockchain as instrumental in engaging in or enhancing data-driven operations.

Chapters "Awareness and Smart City Implementations. Sensing, Sensors, and the IoT in the Public Sector" to "Citizen Participation in Smart Government: A Conceptual Model and Two IoT Case Studies" describe applications, cases, and experiences of IoT in the public sector around the world. In the chapter "Awareness and Smart City Implementations. Sensing, Sensors, and the IoT in the Public Sector", Mckenna explores implementation challenges as opportunities for moving beyond smart and connected governments by focusing on awareness in relation to sensing, sensors, and the IoT in the public sector in the context of smart cities. The chapter is a review of the research literature for smart city implementations, conducted from multiple perspectives and highlighting a range of issues and challenges for the public sector. The theoretical framework for this chapter uses the construct of awareness in relation to the key smart city characteristics of adaptability, complexity, innovation, and readiness. The research design for this work uses a single case study approach to explore evolving understandings of smart city implementations in contemporary urban environments. Multiple methods of data collection are used including surveys and interviews, while content analysis is used in the iterative analysis of data. Data were collected and analyzed from diverse individuals in multiple small, medium, and large sized cities, mostly in Canada. This work makes several contributions by providing (a) an expanded way of looking at IT implementation in the public sector for twenty-first-century urban environments encompassing sensing, sensors, and the IoT; (b) understandings of IT implementation challenges as opportunities in the public sector for more responsive and aware solution-making; and (c) a conceptual framework for more dynamic notions of implementation in the public sector, that is, ambient implementation. This chapter advances an awareness-based explanatory model for ambient implementation of use to the public sector in smart cities.

In the chapter "Use of the Internet of Things in Public Governance for Law Enforcement and Inspection: The Case of Russia", Knutov and Styrin describe how the IoT is being actively introduced in Russian public governance for inspection and oversight. This chapter is based on an analysis of IoT policy, legal acts, secondary statistical data, and the authors' own involvement in testing IoT technologies. They formulate cases and use them as a basis for an IoT classification oriented to the needs of government agencies; the spheres of application considered are transport, justice, retail, and manufacturing. The case studied in greatest detail is the fur industry. They apply the method of cost–benefit analysis and examine the costs of using the IoT in public governance to regulate the turnover of fur goods, as well as the benefits for key stakeholders (government, society, business). As a result, they identify barriers that prevent IoT technology from being used effectively and describe the effects of implementing IoT in the fur industry and other areas in which the IoT is used for inspection and oversight.

In the chapter "The Recognition of the New Digital Entrepreneurs in France: The Case of the French Tech with the Emergence of the Internet of Things", Christophe Premat discusses how since 2014, the question of the implementation of the IoT has been crucial in France. Public authorities have created arenas where digital entrepreneurs and politicians can discuss the evolution of the IoT. In January 2017, the National Assembly published a report on the economic and social consequences of the adaptation of the IoT. This chapter analyzes the political discourse that gives legitimacy to the implementation of the IoT in France. The digital entrepreneurs are the privileged actors of this implementation; their social recognition by the French Parliament and the labelling campaigns (French Tech) reinforces the myth of technological innovation. The field of the critical analysis of discourse is mobilized to evaluate the spread of this new myth in France and the analysis of the legitimization of digital entrepreneurs. This case study reveals how European countries tackle new digital policies in order to control the evolution of the IoT and the field of Artificial Intelligence.

Finally, in the chapter "Citizen Participation in Smart Government: A Conceptual Model and Two IoT Case Studies", Guenduez, Mettler, and Schedler argue that in its simplest form, smart government can be understood as the combination of new technologies and organizational innovation strategies to further modernize the public sector. Within this development, the IoT often forms a key technological foundation, offering government authorities new possibilities for interaction with citizens and local communities. Their chapter "Citizen participation in smart government: A conceptual model and two IoT case studies" argues that on the one hand, citizens can indirectly participate in governmental services' value creation by using public infrastructure or (un)knowingly sharing their data with the community. On the other hand, smart government initiatives may rely more intensively on citizens' active participation to improve public service delivery, increase trust in government actions, and strengthen community sentiment. In this chapter, the authors discuss active and passive participation scenarios of smart government initiatives and explain how sensor-based systems may enhance citizens' opportunities to participate in local governance. They present two practical cases from Switzerland demonstrating these two citizen involvement modes.

Concluding Remarks

As in the private sector, government agencies must engage in continuous improvement if they are to benefit from new and emerging technologies and the paradigm changes they bring. This book responds to the need for new knowledge about the ways in which the latest wave of technology innovations, particularly the IoT, is increasingly integrated in government programs and services and is affecting citizens, businesses, and other social actors. The IoT has the potential to reshape the way government operates and delivers services to citizens. When considering new projects involving the use of the IoT, a flexible and scalable network infrastructure is essential to ensure efficient, reliable, and secure IoT data feeds. Choosing the right network protocols and topologies requires consideration of many different factors, including application needs, coverage requirements, device type and location, power consumption, and budget. Each of these factors can contribute to a different network decision. However, the advancement of the IoT in the public sector depends at least in part on how policymakers and public managers respond to the opportunities and challenges associated with it (Lee 2019). Figure 4 summarizes the main elements, benefits, challenges, and potential applications of the IoT in the public sector.

It is clear that there is no single definition of the IoT and different authors emphasize different aspects of it. In addition, different urban policy domains may require sensors with different features to collect specific types of data, such as electricity or water consumption, air pollution, pedestrian and vehicle movements, or acoustic data from gunshots. Thus, the decision about which smart sensors to use is often

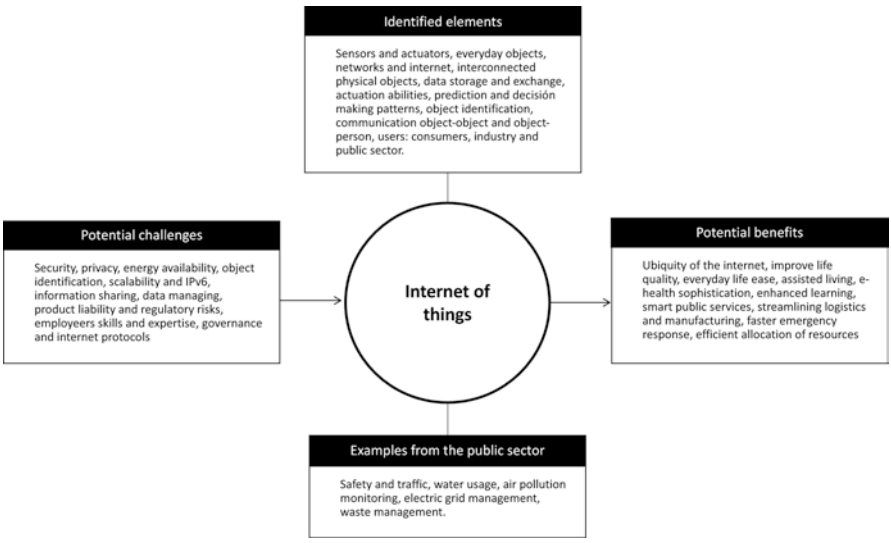


Fig. 4 Summary of IoT benefits, challenges, and potential applications

domain-specific. However, we found some commonalities and practical recommendations in the literature. The initial sensor adoption in one or multiple urban domains is likely to stem from the corresponding functional departments' need to implement their current policies. As a first step in planning for the IoT, it is important to involve people from government programs to identify what existing policies or future programs may drive their imminent needs to use smart sensors and IoT devices (Tang and Ho 2018).

Governments could also foster IoT innovation and deployment by creating effective regulatory environments and policies while removing barriers to IoT adoption (Lee 2019). In his article, Lee (2019, p. 7–8) offers three general governance recommendations for better innovation and implementation of the IoT in the public sector: (1) facilitate interagency coordination, (2) promote public–private partnership, and (3) foster international coordination, collaboration, and engagement.

While the research community on the IoT is fragmented and, to a large extent, focused around single application domains or single technologies (Miorandi et al. 2012), there is opportunity for the fields of public administration, information systems, and digital government to study the IoT as complex socio-technical phenomena. The IoT may create value to users by offering solutions that not only save time and money but could also save lives and help governments allocate resources more efficiently (Lee 2019). Governments could play a role in fostering innovation and removing barriers in order to realize the impact of the IoT on economic growth and social welfare. We are just beginning to see a glimpse of the promising future that the IoT can bring, but we need to understand the challenges and potential limitations in the context of government programs and public policies.

Acknowledgments The authors want to thank Ana Catarrivas for her helpful assistance in the development of the manuscript. This study was partially supported by an internal grant from the University at Albany, State University of New York. The opinions expressed in this chapter are those of the authors and do not necessarily reflect the official views of UAlbany.

References

Alshehri, M. D., Hussain, F. K., & Hussain, O. K. (2018). Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT). *Mobile Networks and Applications*, 1–13.

Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The Social Internet of Things (SIoT)—When social networks meet the Internet of Things: concept, architecture and network characterization. *Computer Networks, 56*(16), 3594–3608.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Bilal, M. (2017). A review of Internet of Things architecture, technologies and analysis smartphone-based attacks against 3D printers. *arXiv preprint arXiv*, 1708.04560.

Brous, P., & Janssen, M. (2015, August). Advancing e-Government using the internet of things: a systematic review of benefits. In International Conference on Electronic Government (pp. 156–169). Springer, Cham.

Brous, P., Janssen, M., & Herder, P. (2018). Internet of Things adoption for reconfiguring decision-making processes in asset management. *Business Process Management Journal*.

Center for Digital Government, CDG. (2017). Get ready because here IoT comes. eRepublic.com

Cho, M. (2015). *South Korea to invest $5b by 2020 in IoT and smart cars, ZDNet*. Retrieved December 19, 2018, from https://www.zdnet.com/article/south-korea-to-invest-5b-by-2020-in-iot-and-smartcars/

Chui, M., Loffler, M., & Roberts, R. (2010). The Internet of Things. *McKinsey Quarterly, 2*, 1–9.

Din, S., Paul, A., Guizani, N., Ahmed, S. H., Khan, M., & Rathore, M. M. (2017). Features selection model for Internet of E-Health things using big data. *GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, 2017* (pp. 1–7). https://doi.org/10.1109/GLOCOM.2017.8254418

El-Haddadeh, R., Weerakkody, V., Osmani, M., Thakker, D., & Kapoor, K. K. (2018). Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2018.09.009.

Erfanmanesh, M., & Abrizah, A. (2018). *Mapping worldwide research on the Internet of Things during 2011-2016*. The Electronic Library, https://doi.org/10.1108/EL-09-2017-0196. Permanent link to this document: https://doi.org/10.1108/EL-09-2017-0196

Gascó, M. (2017). *Capítulo 9 Ciudades y gobiernos inteligentes: Un fenómeno en auge. Tecnologías de Información y Comunicación en la Administración*. Mexico: Infotec.

Gohar, M., Ahmed, S. H., Khan, M., Guizani, N., Ahmed, A., & Rahman, A. U. (2018). A big data analytics architecture for the Internet of Small Things. *IEEE Communications Magazine, 56*(2), 128–133.

Gil-Garcia, J. R., Pardo, T. A., & Aldama-Nalda, A. (2013, June). Smart cities and smart governments: using information technologies to address urban challenges. In *Proceedings of the 14th Annual International Conference on Digital Government Research* (pp. 296–297). New York: ACM.

Harbert, T. (2017). *Practical uses of the Internet of Things in government are everywhere, government technology*. Retrieved from http://www.govtech.com/network/Practical-Uses-of-the-Internet-of-Things-in-Government-Are-Everywhere.html

Hatem, B. E. N., Rejeb, A. B., & Gattoufi, S. (2016, August). Dealing with imperfect data in "Smart-Cities". In *Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research, PhD Papers, Posters and Workshops of IFIP EGOV and EPart 2016* (Vol. 23, p. 211). Amsterdam: IOS Press.

Hernández-Ramos, J. L., Pérez, S., Hennebert, C., Bernabé, J. B., Denis, B., Macabies, A., & Skarmeta, A. F. (2018). Protecting personal data in IoT platform scenarios through encryption-based selective disclosure. Computer Communications, 130, 20–37.

INFSO. (2008). D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems. In *Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008*.

Jaafreh, A. B. (2018). The effect factors in the adoption of Internet of Things (IoT) technology in the SME in KSA: An empirical study. *International Review of Management and Business Research, 7*(1), 135–148.

Jesus, E. F., Chicarino, V. R., de Albuquerque, C. V., & Rocha, A. A. D. A. (2018). A survey of how to use blockchain to secure Internet of Things and the stalker attack. *Security and Communication Networks,* 2018, https://doi.org/10.1155/2018/9675050

Johannessen, M. R., & Berntzen, L. (2016). Smart cities through implicit participation: using gamification to generate citizen input for public transport planning. In H. J. Scholl et al. (Eds.), *Electronic government and electronic participation*. Amsterdam: IOS Press. https://doi.org/10.3233/978-1-61499-670-5-23.

Kadarina, T. M., & Priambodo, R. (2017, November). Preliminary design of Internet of Things (IoT) application for supporting mother and child health program in Indonesia. In *2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP)* (pp. 1–6). New York: IEEE.

Keskin, T., & Kennedy, D. (2015, January). Strategies in smart service systems enabled multi-sided markets: Business models for the internet of things. In *2015 48th Hawaii International Conference on System Sciences (HICSS)* (pp. 1443–1452). New York: IEEE.

Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2010). Smart objects as building blocks for the internet of things. *IEEE Internet Computing, 14*(1), 44–51.

Lakshmi, I. (2018). A vision, architectural elements, and future direction of Internet of Things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(1), 477–328.

Latif, S., Mahfooz, S., Ahmad, N., Jan, B., Farman, H., Khan, M., et al. (2018). Industrial Internet of Things based efficient and reliable data dissemination solution for vehicular Ad Hoc networks. *Wireless Communications and Mobile Computing, 2018*.

Lee, G. (2019). What roles should the government play in fostering the advancement of the internet of things?. Telecommunications Policy, 43(5), 434-444.

Lee, S., Choi, M., & Kim, S. (2017). How and what to study about IoT: Research trends and future directions from the perspective of social science. *Telecommunications Policy, 41*, 1056–1067.

Lin, C., Chuang, S., Lin, S., & Lin, C. (2017). A healthcare on demand device by using internet of things for elderly center. *DEStech Transactions on Computer Science and Engineering, (Proceedings ICEITI 2017)*.

Liu, Z., Choo, K. K. R., & Grossschadl, J. (2018). Securing edge devices in the post-quantum internet of things using lattice-based cryptography. *IEEE Communications Magazine, 56*(2), 158–162.

Lopez, G. (2013). *An introduction of Internet of Things (IoT)*. San Francisco. Retrieved November 7, 2017, from https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf.

Mershad, K., & Wakim, P. (2018). A learning management system enhanced with Internet of Things applications. *Journal of Education and Learning, 7*(3), 23.

Middha, K., & Verma, A. (2018). Internet of things (IOT) architecture, challenges, applications: A review. *International Journal of Advanced Research in Computer Science*, *9*(1).

Middleton, P., Kjeldsen, P., & Tully, J. (2013). "Forecast: The Internet of things, worldwide, 2013," gartner analysis report ID: G00259115.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.

OECD. (2014). *Technology foresight forum*. https://www.oecd.org/sti/ieconomy/technology-foresight-forum-2014.htm

Pal, D., Funilkul, S., Charoenkitkarn, N., & Kanthamanon, P. (2018). Internet-of-things and smart homes for elderly healthcare: An end user perspective. *IEEE Access*, 6, 10483-10496.

Perera, C., Jayaraman, P. P., Zaslavsky, A., Georgakopoulos, D., & Christen, P. (2014, January). Mosden: An internet of things middleware for resource constrained mobile devices. In *2014 47th Hawaii International Conference on System Sciences (HICSS)* (pp. 1053–1062). New York: IEEE.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by internet of things. *Transactions on Emerging Telecommunications Technologies, 25*(1), 81–93.

Perez, A. J., Zeadally, S., & Cochran, J. (2018). A review and an empirical analysis of privacy policy and notices for consumer Internet of Things. *Security and Privacy*, e15. https://doi.org/10.1002/spy2.15.

Raffman, M. S., & Russo, A. H. (2018). Mitigating transactional risk in the Internet of Things. *The Journal of Private Equity, 21*(2), 65–73.

Rajguru, S., Kenhekar, S., & Pati, S. (2015). Analysis of IoT in a small environment. *The International Journal of Advanced Networking and Applications, 4*(4), 2015.

Savner, M., & Gugapriya, G. (2018). Train collision avoidance system for automatic train protection using Internet of Things. In *Intelligent Embedded Systems* (pp. 115–127). Singapore: Springer.

Sedrati, A., & Mezrioui, A. (2018). A survey of security challenges in Internet of Things. *Advances in Science, Technology and Engineering Systems Journal, 3*(1), 274–280.
Sen, A. A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: A survey. *International Journal of Information Technology*, 1–12.
Sivakumar, D., Jusman, M. F. B., & Mastan, A. N. B. M. (2017). A case study review: Future of Internet of Things (IoT) in Malaysia. In *ASCENT International Conference Proceedings – Information Systems and Engineering, 23-24, November 2017*.
Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commission, 3*(3), 34–36.
Tang, T., & Ho, A. T. K. (2018). A path-dependence perspective on the adoption of Internet of Things: Evidence from early adopters of smart and connected sensors in the United States. Government Information Quarterly. Retrieved October 6, 2018.
The Economist Intelligence Unit. (2013). *The Internet of Things Business Index, A quiet revolution gathers pace*. Retrieved August 29, 2016, from http://www.arm.com/files/pdf/EIU_Internet_Business_Index_WEB.PDF
Thibaud, M., Chi, H., Zhou, W., & Piramuthu, S. (2018). *Internet of Things (IoT) in high-risk environment. Health and Safety (EHS) industries: A comprehensive review. Decision Support Systems*. Retrieved February 25, 2018.
Wakefield, K. J. (2014). *How the Internet of Things is transforming manufacturing*. Forbes. Retrieved November 30, 2018, from http://www.forbes.com/sites/ptc/2014/07/01/how-the-internet-of-things-istransforming-manufacturing/#1e76c898228e.
Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). How 'big data'can make big impact: Findings from a systematic review and a longitudinal case study. International Journal of Production Economics, 165, 234–246.
Werthmuller, D. (2016). *The IoT challenge for local governments as data stewards*. Albany, NY: The Research Foundation of State University of New York.
Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261–274.
Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems, 25*(9), 1101.
Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.
Zeng, D., Guo, S., & Cheng, Z. (2011). The Web of Things. *Journal of Communications, 6*(6), 424–438.

J. Ramon Gil-Garcia is an Associate Professor of Public Administration and Policy and the Research Director of the Center for Technology in Government, University at Albany, State University of New York (SUNY). Dr. Gil-Garcia is a member of the Mexican Academy of Sciences and of the Mexican National System of Researchers as Researcher Level III, which is the highest distinction a researcher can obtain before becoming Researcher Emeritus as a result of a lifelong career of research contributions. In 2009, he was considered the most prolific author in the field of digital government research worldwide, and in 2013 he was selected for the Research Award, which is "the highest distinction given annually by the Mexican Academy of Sciences to outstanding young researchers." More recently, Dr. Gil-Garcia was named one of the "World's 100 Most Influential People in Digital Government in 2018" by Apolitical, which is a nonprofit organization based in London in the United Kingdom. Currently, he is also a professor of the Business School at Universidad de las Américas Puebla in Mexico, a Faculty Affiliate at the National Center for Digital Government, University of Massachusetts Amherst, and an Affiliated Faculty member of the Information Science Doctorate Program at the College of Engineering and Applied Sciences, University at Albany. Dr. Gil-Garcia is the author or co-author of articles in prestigious international journals in Public Administration, Information Systems, and Digital Government and some

of his publications are among the most cited in the field of digital government research worldwide. His research interests include collaborative electronic government, inter-organizational information integration, smart cities and smart governments, adoption and implementation of emergent technologies, information technologies and organizations, information technologies and education, digital divide policies, new public management, public policy evaluation, and multi-method research approaches. Dr. Gil-Garcia has extensive teaching experience and has collaborated with 11 universities, including departments of Public Administration, Political Science, Social Science, Information Studies, and Management Information Systems. Dr. Gil-Garcia also has many years of experience as a consultant for federal, state, and local government agencies.

Theresa A. Pardo is Director of CTG UAlbany, an applied research institute at the University at Albany, State University of New York, where she is also a full research professor in Rockefeller College of Public Affairs and Policy. CTG UAlbany works closely with multi-sector and multi-disciplinary teams from the U.S. and around the world to carry out applied research and problem solving projects focused on the intersections of policy, management, and technology in the governmental context. Dr. Pardo serves as OpenNY Adviser to New York State's Governor Andrew Cuomo and is Chair of the U.S. Environmental Protection Agency's National Advisory Committee. She serves as a member of the User Working Group of the NASA Socioeconomic Data and Applications Center (SEDAC), the Business and Operations Advisory Committee of the U.S. National Science Foundation and the Steering Committee of the U.S. National Science Foundation funded North East Big Data Innovation Hub. Dr. Pardo is founder of the Smart Cities, Smart Government Research-Practice Global Consortium and a Past-President of the Digital Government Society. In 2018, Dr. Pardo was named as one of the Top 100 Influencers in Digital Government globally. She is also a recipient of Government Technology Magazine's Top 25 Doers, Drivers, and Dreamers Award which recognizes individuals throughout the U.S. who exemplify transformative use of technology that's improving the way government does business and serves its citizens. Dr. Pardo is a recipient of the University at Albany's Distinguished Alumni Award, the University at Albany's Excellence in Teaching Award, and the Rockefeller College Distinguished Service Award. Dr. Pardo holds a Ph.D. in Information Science from the University at Albany, SUNY.

Mila Gasco-Hernandez holds an MBA and a Ph D in Public Policy Evaluation (Award Enric Prat de la Riba granted to the best Ph D thesis on public management and administration, given by the School of Public Administration of Catalonia in Barcelona, Spain). She is the Associate Research Director of the Center for Technology in Government as well as a Research Associate Professor at the Rockefeller College of Public Affairs and Policy, both at the University at Albany—SUNY. Before joining SUNY, Dr. Gasco-Hernandez served as a senior researcher at the Institute of Governance and Public Management (currently known as ESADEgov—Center for Public Governance) and the Institute of Innovation and Knowledge Management, both at ESADE Business and Law School in Spain. Previous to that, she was a senior analyst at the International Institute on Governance of Catalonia and a professor in Rovira i Virgili University and Pompeu Fabra University, both in Spain.

Mila Gasco-Hernandez has considerable consulting experience on the information and knowledge society as well. In this respect, she has worked for a wide variety of organizations such as the United Nations Development Programme, the Mayor's Office in Valencia (Venezuela), the Spanish Agency for International Development Cooperation, the City Council and the Provincial Council of Barcelona, the International Institute for Democracy and Electoral Assistance, the Latin American Centre on Management for Development (for whom she co-developed the Ibero-American Interoperability Framework), the World e-Governments Organization of Cities and Local Governments (she was the leading judge for the WeGo Awards), the Inter-American Development Bank, or Google.

Her areas of research are mainly related to information and technology in government and, among others, they include electronic and open government, e-governance, public sector innovation, smart cities, and public policy evaluation.

The Internet of Things in a Smart Society: How Government Policy Can Help Seize Opportunities and Mitigate Threats

Ronald Pool, Jasper van Berkel, Susan van den Braak, Maaike Harbers, and Mortaza S. Bargh

Abstract The IoT is a revolutionary development for both society and governments. In this chapter opportunities and threats of the IoT are discussed. Linking technological, societal, economic, and policy-oriented aspects of the IoT, this chapter introduces a conceptual framework to map and analyze the factors or obstacles that arise in addressing IoT opportunities and threats, and possible government measures to mitigate these factors. By adopting a broad view and paying attention to the relations between different factors, this chapter shows that there is no one-size-fits-all solution for IoT-related issues, as different problems and solutions are interdependent and require a coherent government approach.

Keywords Internet of Things · Opportunities · Threats · Human and societal values · Government measures

R. Pool
ICTRecht, Amsterdam, The Netherlands
e-mail: r.pool@ictrecht.nl

J. van Berkel · S. van den Braak (✉)
Research and Documentation Centre, Ministry of Justice and Security, Den Haag, The Netherlands
e-mail: j.j.van.berkel@minvenj.nl; s.w.van.den.braak@minvenj.nl

M. Harbers
Research Centre Creating 010, Rotterdam University of Applied Science, Rotterdam, The Netherlands
e-mail: m.harbers@hr.nl

M. S. Bargh
Research and Documentation Centre, Ministry of Justice and Security, Den Haag, The Netherlands

Research Centre Creating 010, Rotterdam University of Applied Science, Rotterdam, The Netherlands
e-mail: m.shoae.bargh@minvenj.nl; m.shoae.bargh@hr.nl

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*, Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_2

Abbreviations

CE	Conformité Européenne
CLTC	Center for Long-term Cybersecurity
GDPR	General Data Protection Regulation
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information technology
R&D	Research and development
SWOT	Strengths, weaknesses opportunities, threats

Introduction

The Internet of Things (IoT) will play an increasingly prominent role in everyday life. It is estimated that the IoT will contain 20–30 billion objects in 2020 (Gartner 2015; WEF 2015), where "objects" can range from toothbrushes and lamps to animals and humans (with implants), from cars and houses to energy networks and cities. It will therefore have a major impact on many aspects of society, such as employment, healthcare, transportation, and prosperity (Atzori et al. 2010; Borgia 2014; Whitmore et al. 2015; Al-fuqaha et al. 2015).

Technological developments, such as the IoT, will also influence governments and public policy (GO-Science 2014). With an increasing amount of connected devices containing sensors, more and more data will be collected and exchanged. As a result, more relevant and real-time information will be available (Whitmore et al. 2015). By combining, analyzing, and interpreting these data, processes can become more transparent and new insights can be obtained. This can help governments to make better and more informed decisions.

The use of technologies to facilitate government activities has long been discussed, using concepts such as e-government, digital government, and smart government (Layne and Lee 2001; Moon 2002; West 2004; Gil-Garcia et al. 2014; Janowski 2015). The scope of each concept differs. Some authors limit the scope to the use of technology for daily public administration (Moon 2002) or to government services delivered by digital means (West 2004). In a broader sense, it could be seen as a "creative mix of emergent technologies and innovation in the public sector" (Gil-Garcia et al. 2014: 17).

Regardless of the scope, it is clear that the IoT will influence these concepts. This chapter uses a scheme of human and societal values, as a way to address the opportunities and threats of the IoT. It should be noted that the notion of values has been used as a framework of categorization and should not be interpreted as a theoretical approach. The starting point of our categorization was the idea that technology has an impact on human values (Friedman et al. 2013). Some values are positively affected by the IoT and others are negatively affected, constituting both opportunities

and threats. The public sector plays a vital role in seizing these opportunities and mitigating the threats. In this chapter we offer a conceptual framework for understanding, framing, and approaching the factors that arise in addressing both opportunities and threats.

The outline of the chapter is as follows. Section "Related work" discusses related work on opportunities and threats of the IoT in specific domains and IoT regulation. Section "Approach" discusses our approach and methodology. Section "IoT Opportunities and Threats" provides an overview of the opportunities and threats posed by the IoT. Section "Government Measures" introduces a conceptual framework including factors and government measures for addressing the opportunities and threats. Section "Conclusion" provides a conclusion.

Related Work

This chapter aims to provide a broad overview of IoT-related issues, including its opportunities and threats, possible measures that allow society to benefit from the IoT, and the role of the public sector in particular. While doing so, the chapter brings together scientific research, professional literature, news articles, and expert opinions. This wide perspective distinguishes this work from most other contributions on this topic, which often concentrate on a specific application domain or a narrower problem related to the IoT. Related work focuses on, for example, opportunities and challenges of the IoT in healthcare (Fernandez and Pallis 2014) and industries (Da Xu et al. 2014), security concerns (Sicari et al. 2015; Xu et al. 2014), privacy concerns (Sicari et al. 2015), or issues in relation to big data (Sun et al. 2016). There are a number of papers that discuss the opportunities and threats of the IoT in general (e.g., Davies 2015; Rose et al. 2015), but these only shortly discuss the possible measures needed for overcoming the challenges and supporting the opportunities.

Besides having a broader focus, this chapter distinguishes itself from other contributions by providing an analysis of the obstacles that hinder the implementation of IoT-related measures to seize opportunities or mitigate threats. Other institutes (GO-Science 2014; CSR 2016a) published their reports proposing some measures for mitigating IoT challenges. However, they fail to explicate the relations between different measures and the relations of those measures to the fundamental obstacles in implementing them. The obstacles that are discussed in this chapter are brought up in some other papers as well. For example, Danezis et al. (2014) and Peppet (2014) mention some obstacles like lack of governance, incentives, and knowledge. However, they neither provide the relations between different obstacles nor between obstacles and solution directions.

This work is one of the few that links technological, societal, economic, and policy-oriented aspects of the IoT. By adopting a broad view and paying attention to the relations between different issues, this chapter shows that there is no one-size-fits-all solution for IoT-related issues, as different problems and solutions are

interdependent and require a coherent approach. Our work has focused on the situation in the Netherlands, but we expect that many of the findings are applicable to other (developed) countries as well.

Approach

The research presented in this chapter was performed in two phases. First, we made an overview of the opportunities and threats of the IoT. Second, we investigated which measures need to be taken to seize these opportunities and mitigate the most important threats. In this process, we used the notion of "values" as a conceptual tool for mapping, describing, and analyzing the opportunities and threats, and determining which measures to take. Again, it is important to note that these "values" are not used as a theoretical foundation for analyzing the opportunities and threats.

This approach is founded on the idea that people's values guide what they consider important in life, what judgments they make about the world, and how they act in specific situations. Likewise, in governance, all policy decisions are underpinned by values, even though they often remain implicit (Chang 1997; Kooiman and Jentoft 2009). It has been argued that making values explicit can help making policy decisions. Song and colleagues, for example, state that "governance challenges could be lessened if stakeholders' values, images, and principles are made explicit, understood, and articulated into the policy and decision-making process" (Song et al. 2013: 1). The concept of responsible innovation (adopted, among others, by the European Commission), which looks at the potential impact on society and environment of an innovation process, also takes values into account (Stilgoe et al. 2013). For these reasons, we deemed the framework of values suitable to map the opportunities and challenges of the IoT.

In the first phase of our research we assessed which human and societal values are affected most by the rise of the IoT. Generally, technological developments have both positive and negative impacts, constituting opportunities and threats, respectively. For example, a smart grid can decrease energy consumption and thus support the value of sustainability—an opportunity. Yet the smart meters needed for such a solution may violate one's privacy—a threat.

We collected information about values and the IoT through the following methods: (1) desk research, (2) interviews, and (3) roundtable discussions. Desk research was performed using a selection of fixed search terms to search for available scientific literature in Google Scholar. Based on these initial results we expanded our search by using a snowball method, which enabled us to find additional literature that seemed relevant for our study. As many of the developments are recent and new we also included media articles in our literature survey. Next to the desk research, two themed roundtables were organized to discuss Smart Cities and Smart Industry using a SWOT analysis. To supplement these findings a total of six semi-structured interviews were conducted with various experts and stakeholders from different sectors. We used the results from this research to categorize the potential positive

and negative effects of the IoT according to the "value at stake," giving priority to those effects that were mentioned multiple times. This resulted in a list with positively affected values—opportunities, and a list with negatively affected values—threats, as described in Section "IoT Opportunities and Threats". It is important to note that these lists are by no means exhaustive, but rather, form a useful taxonomy to describe the societal and economic opportunities and threats of the IoT.

In the second phase, the most important opportunities and threats identified in the first phase were taken as a starting point to identify measures for seizing and mitigating them. They were selected from all measures that came up in the desk research, interviews and roundtables. Again, we paid attention to those measures that were emphasized or mentioned multiple times. We also identified the possible relations and interdependencies between different measures and their corresponding solution directions. This phase resulted into two insightful diagrams that also illustrate the relations among the various measures (see Section "Government Measures").

IoT Opportunities and Threats

This section presents the positive and negative effects of the IoT on different human and societal values in Sections "IoT Opportunities" and "IoT Threats", respectively.

Opportunities

As is discussed in the introduction, data produced and exchanged by the IoT can improve understanding and transparency, which can contribute to better decisions by businesses and governments. As a result, the IoT can have a strong positive impact on the following values: well-being, sustainability, productivity and prosperity, which prominently arose in our desk research and interviews. The positive impact of the IoT on these values is discussed below.

Well-Being

The IoT can contribute to well-being in several ways. Firstly, it can improve quality of life by automating processes in daily life. IoT applications can make cities more accessible and more attractive to citizens by, for example, optimizing the flow of traffic, monitoring the availability of parking spaces, and improving garbage disposal routes (Miorandi et al. 2012; Pandya & Champaneria 2015; Whitmore et al. 2015; Zanella et al. 2014). Secondly, it can be used to improve the health of users. Wearables, for instance, can help people to adopt a healthy lifestyle by improving their movement, sleeping and eating patterns (Beaudin et al. 2006; Kong et al. 2012;

Silver et al. 2012; Swan 2013). The IoT can also assist people with a visual, auditory, or physical impairment (Domingo 2012), or the IoT devices can be used to monitor at-risk patients (Healey et al. 2015). Finally, it can contribute to well-being by making people's surrounding and the public domain safer. The IoT can monitor homes and detect break-ins, smoke, or flooding. The same sensors could also be used in the public domain and assist law enforcement (Farooq et al. 2015; Miorandi et al. 2012). Smart lampposts could, for example, detect noise and possible criminal behavior.

Sustainability

The IoT can help sustainability in several ways. Firstly, applications in homes provide ways for consumers to save on energy and water usage. Smart meters and thermostats provide real-time feedback on energy usage, and they can automatically adjust heating. Secondly, IoT applications in cities can provide insight into the energy use of public services, and help to optimize it (Zanella et al. 2014). IoT sensors can also monitor the air quality in cities (Farooq et al. 2015; Miorandi et al. 2012; Zanella et al. 2014) and based on that, for example, automatically redirect cars when certain limits are exceeded. Thirdly, energy networks can be turned into smart grids by embedding sensors in them, increasing their efficiency, security, and reliability (Wang et al. 2012; Yan et al. 2013; Borgia 2014). Smart grids make it possible to detect malfunctions in the network at an earlier stage, and to better balance the supply and demand of energy. Increasingly, this will also extend to homes, for example, by temporarily storing and discharging energy in electric cars, depending on the needs of the network (Yan et al. 2013). Lastly, the IoT could also contribute to the circular economy by providing insight in the use of energy and resources during the lifetime of a product (Ellen MacArthur Foundation 2016). In the wake of the Paris climate agreements, this can contribute to achieving their objectives.

Productivity

The IoT can increase productivity by making predictions, optimizing processes and taking decisions. A few examples of applications in logistics, manufacturing, and agriculture are discussed below. In the logistics sector, RFID chips are used to track products through the entire supply chain. This helps optimizing the supply chain, for example, by maintaining smaller inventories (Atzori et al. 2010; Whitmore et al. 2015). Manufacturing processes can also be optimized through real-time access to information (Atzori et al. 2010; Stratix 2015), for instance by performing preventive maintenance (Atzori et al. 2010; Al-Fuqaha et al. 2015; Borgia 2014). In agriculture, the IoT can advance precision agriculture, in which crops and animals are closely monitored and treated. It can monitor soil and crop properties, weed densities, and diseases and pests (Bos and Munnichs 2016). Livestock farmers can also use the IoT to monitor the performance of animals individually, for example with

respect to milk yields, fertility and possible diseases (Bos and Munnichs 2016). It is expected that IoT use will be vital for companies and countries to stay competitive in the future.

Prosperity

Estimations of the potential economic impact of the IoT range from $1.9 trillion to as much as $14.4 trillion annually (Bradley et al. 2013; Lund et al. 2014; Manyika et al. 2013; GO-Science 2014). Despite this discrepancy in predictions it is clear that the IoT will have a big impact on the economy. In part, this will be due to the availability of a whole range of physical IoT products (e.g., sensors) that provide opportunities for companies to innovate and develop new products. Besides that, the IoT will impact services. IoT products, data and software will be sold as a service by offering subscription-based access to products, data and software (Castermans et al. 2014; CPB and PBL 2015; Frenken 2015). Many physical IoT products will be accompanied with complementary services. For example, some smart thermostats already come with services that give users additional information on how to optimize their energy usage. Finally, the IoT will improve existing services, for example, by offering preventive maintenance (Smit et al. 2016), by giving personalized offers, or by providing information about product availability to consumers in stores (Gregory 2015). Traditional business models of one-off deals are thus transformed into a situation in which products generate revenue over their entire lifetime.

The IoT will also have a big impact on the job market. Historically, technological revolutions have been positive for the job market. Although certain types of jobs disappeared, technological developments have also created new jobs (Van Est and Kool 2015; Went and Kremer 2015). Such a shift offers opportunities for people and businesses with the right expertise. With an aging population and a shrinking workforce, the IoT offers opportunities to maintain economic growth by replacing certain jobs (as demand for labor exceeds supply), and by improving labor productivity, often seen as an important prerequisite for economic growth (Van Est and Kool 2015).

Threats

The previous section described various opportunities and possibilities that the IoT offers by collecting large amounts of (sensor) data. However, collecting such large amounts of data and increasing the use of connected devices also have a downside. This section will describe how the following values, as identified in our desk research and interviews, are threatened by the advent of the IoT. These values are security and safety, privacy, prosperity, well-being, equality, and autonomy.

Security and Safety

As the number of objects connected to the IoT increases, so too will the number of security and safety risks and their impacts. Therefore, lack of an adequate level of security and safety is one of the main concerns regarding the IoT (Goodman 2015; FTC 2015; Peppet 2014). A security risk is an intentionally caused risk, for example, the risk associated with a system attack carried out intentionally by malicious people (Aoyama et al. 2013). Security risks affect the confidentiality, integrity, and availability of devices (Mattord 2014). For example, by rendering the device unavailable with ransomware (Goodman 2015; Williams 2016) or affecting its integrity by adjusting or deleting sensor data (Koebler 2015).

Safety risks, on the other hand, occur due to, for example, human errors, design errors, or malfunctions without explicit intentions (Aoyama et al. 2013). These risks can be caused by faulty hardware, such as malfunctioning sensors, glitches in the underlying infrastructure, or emergent behavior between interconnected devices (Roca et al. 2016).

At this point in time, it is noteworthy that few mitigation measures are being taken to reduce security and safety risks. Moreover, basic security measures like avoiding default usernames and passwords are often not taken by companies, making hacking of IoT devices considerably easier. For example, the Mirai botnet consisted of thousands of IoT devices that were hacked because of this vulnerability (Krebs 2016). Because of the disruptive impact that insecure or unsafe devices will have on society, taking security and safety measures will become an increasingly important policy topic.

Privacy

As described above, IoT applications collect large amounts of data. These data can often be traced back to specific people and their use may violate these people's privacy. The anonymization of personal data collected by IoT devices proves to be problematic (Peppet 2014). Moreover, by combining and editing apparently "innocent" data, sometimes new sensitive personal data can be created (Rose et al. 2015; Hildebrandt 2008; WRR 2016). For example, combining and analyzing data on heart rate and acceleration can result in data on stress levels, happiness, or overall health of users (Peppet 2014).

Another privacy-related risk is automated decision-making based on sensor data. Several authors point out that this could lead to social exclusion and discrimination (Custers et al. 2013; Peppet 2014; Zarsky 2014, 2016). Furthermore, data collected could end up being used for different IoT applications, without people being aware of it (WRR 2016). The IoT also offers opportunities for government agencies to collect data (Ackerman and Thielman 2016). IoT applications enable continuous monitoring of individuals and therefore are particularly suited for police surveillance and spying purposes. For example, through microphones in CCTV cameras, an act of aggression can be identified using special software (Flight 2016). It is also possible for a retailer

to count the number of people by measuring Wi-Fi and Bluetooth signals (WRR 2016). The above applications may violate the right to privacy in a variety of ways and could have a "chilling effect," as people tend to adjust their behavior according to a new (or alleged) measure (Kaminski and Witnov 2015).

Current legislation in Europe, such as the General Data Protection Regulation (GDPR) requires the purpose of data processing to always be clear in advance. However, for IoT applications this has proven not to be the case. This could lead to a "function creep," where data is used for a different purpose than it was originally collected for (WRR 2016). Furthermore, many applications will use big data analyses, in which generally all available data are analyzed and the outcome of the analysis is often not clear in advance (Zwenne 2015). Lastly, informed consent will be challenged as devices without a screen make it difficult for users to view the privacy settings (Peppet 2014) and to allow unequivocal permission for data processing (Zwenne 2015). Above examples show that the IoT will introduce many potential privacy issues that will need to be addressed in the future.

Prosperity

Over the past twenty years, technological developments have contributed significantly to prosperity and economic growth (Van Est and Kool 2015). While opinions on the relationship between employment and the robotization of society differ (Van Est and Kool 2015; Arntz et al. 2016), it is clear that technological advancements are likely to affect both job market and business competitiveness. The IoT creates new markets and opportunities, but if companies fail to respond in time, they may no longer be able to compete with international companies. Some companies have difficulty responding to the new "online reality," which, with the advent of the IoT, is about to increase even more. These digital platforms are new technology-driven business models, often with a winner-takes-all mentality (Van Est and Kool 2015; Bijlsma et al. 2016). Emerging IoT-enabled services may diminish the market share of those players that do or cannot timely embrace the opportunities. Some authors (Van Est and Kool 2015; Bijlsma et al. 2016) warn that these digital platforms may lead to the so-called platform capitalism, in which one or two parties are dominant in a certain sector. Related to this, a lack of standards for IoT services and systems affects the interoperability and durability of IoT devices and services. There is a risk that IoT devices that are purchased now will become unusable because the existing specifications are no longer supported. This problem plays on an international level and therefore requires collaboration between governments on a global scale. In this global context, it is noteworthy to mention the development of standards for smart cities with the ISO 37120:2014.[1] This is the first ISO standardization of city data, defining 100 city performance indicators. Measuring the performance of a city can be seen as a fundamental aspect of a smart city.

[1] https://www.iso.org/standard/62436.html.

Well-Being

Technological advancements of the IoT can threaten the general well-being of our society in a number of ways. Firstly, as the IoT collects large amounts of data, people have access to and also share a lot of information. To make sure all this information does not overwhelm its users, IoT applications also help to process and interpret it. To that end, Weiser and Seeley-Brown (1995) suggest that "the way to become attuned to more information is to attend to it less". When IoT applications fall short in this regard, it could lead to an information overload, concentration issues and stress (Wurman 1989), as people have difficulties handling large amounts of information (Bawden and Robinson 2009).

Secondly, autonomous devices may limit our freedom of choice. Advanced algorithms can, for instance, determine when to turn on your lights or central heating systems, and how to drive your car to a specific destination. Consequently, it becomes more difficult for users to influence the system's decisions (Amichai-Hamburger 2002) and to completely evade IoT applications and not share personal information (Peppet 2014).

Lastly, the rapid growth of the IoT comes with some new developments of which the effects are not yet fully known. One of these developments is the fact that technology can have a negative impact on social interactions. In literature it is argued that with increased use of technology, morality is divided between humans and technology (Van den Berg and Keymolen 2013). This could lead to a reduction of critical reflection on our actions and a reduced moral awareness of people (Keymolen 2014). Technology philosophers also point out that people are becoming increasingly fused with technology, which fades the boundary between human and technology (Floridi 2015; Verbeek 2011).

Government involvement may contribute to emphasizing the importance of this human value in societal development.

Equality

Technological progressions have led to a gap between those who can benefit from digital technologies and those who cannot (Norris 2001), which can result in impending equality. The arrival of the IoT threatens to increase the digital divide. Those individuals who cannot benefit from new technologies are subjected to the increasing threat of being excluded from (public) services because they are unable to use digital resources (effectively). For example, it is plausible that insurance premiums would go down for people with a smart home or smart car in the near future. Furthermore, some warn that certain areas or neighborhoods not connected to the IoT will run the risk of being excluded from certain public services (CLTC 2016). Lastly, economical changes could also lessen equality in the workforce when it comes to salary, working conditions, and job opportunities (Roose 2014; Van Est and Kool 2015).

Autonomy

The more dependent society is on technology, the greater are the consequences of technological failures. This increasing reliance on technology, which is enhanced by the rise of the IoT, poses a threat to our autonomy in several ways. Firstly, it creates a risk of failure of IoT devices due to Internet and power outage, or due to an overload of communication networks. Infrastructure failures will affect an increasing number of devices and technologies. Secondly, with an increased reliance on technology, knowledge, and skills could be lost as they are no longer needed. This, in turn, increases the impact of possible technological failures (Pereira et al. 2013; Lu 2016).

In addition to the risk of technical malfunctions, a growing IoT also creates new dependencies on manufacturers. This can cause safety hazards, for example, because software and hardware vulnerabilities/leaks are no longer patched. The dependency on manufacturers may also harm national interests. The CLTC (2016) outlines a future in which countries nationalize IoT production to counter potential spying or tampering efforts from other countries. The CLTC predicts that a number of large networks will emerge from countries such as China and the United States. Small countries in particular will have to choose which area of influence they want to belong to. This raises all kinds of questions about, for example, the impact these countries will have on the produced (privacy-sensitive) data, and the role governments should play in this process.

Summary and Analysis

The previous sections have shown that the IoT will have a big impact on our society, with both positive and negative consequences for different human values. The extent to which these consequences will affect society depends on the ways in which the IoT will be used, developed, and regulated. As these human values are closely aligned with public policy goals, IoT developments should be taken into account when creating (new) policy.

Considering all values that are positively affected by the IoT, we see IoT-driven economic growth as the biggest opportunity of the IoT because it will have the biggest impact on society. It affects many of the values discussed in Section "Opportunities", which, in turn, also contribute to economic growth. For example, sustainability benefits not only the environment but also the economic growth, by offering new sustainable products and services. The IoT can also help to lower costs because, for example, the elderly can live at home longer or because healthcare costs decrease.

Regarding threats, we consider risks related to cybercrime (security), dysfunctional IoT devices (safety), and the invasion of privacy as the biggest threats. To a certain extent, this also relates to the other values discussed in Section "Threats". Government policy can play a more significant role in the values of prosperity and

the loss of autonomy; where the negative consequences of something going wrong will grow as we get more dependent on technology.

Lastly, it is important to note that not addressing the opportunities or threats can lead to physical, social, or economic damage. However, when both the opportunities and threats are addressed, it can positively affect economic growth and other values. Thus, there is a positive interaction between stimulating economic growth and taking security measures. This means that only focusing on one aspect will limit the potential benefits the IoT can have.

Government Measures

Although businesses are mainly in a leading position to take initiatives for seizing IoT opportunities and mitigating its threats, governments can encourage companies to take actions through policies. In fact, in this section we will show that the government plays a crucial role in ensuring a profitable and safe IoT. An overview of possible government measures to stimulate economic growth, as the main positive consequence of the IoT, and mitigate security, safety, and privacy risks, as the main negative consequences of the IoT, is provided below.

Economic Growth

Figure 1 shows a summary of the factors and the associated (government) measures that can positively affect economic growth. These *factors* (dark grey blocks) can be divided into (1) boosters of economic growth and (2) conditions for economic growth, as indicated in Fig. 1. This classification is based on a conceptual model of Statistics Netherlands (CBS 2013). In this section we use this model to discuss *measures* (light grey blocks) that can contribute to economic growth due to the IoT. The figure shows that preventing security and privacy-related risks is an important requirement for promoting economic growth. Measures to mitigate these risks are discussed in Section "Security, Safety and Privacy".

Human Capital and Workforce

Human capital and workforce are associated with knowledge and skills of the workforce (CBS 2013). The IoT as well as the further digitization of the economy requires a workforce with sufficient IT skills. This also applies to businesses and governments, which need sufficient knowledge to develop new products, services, and policies. Previous research shows that there is currently a shortage of IT knowledge in the country's workforce as well as in organizations (Van Lakerveld et al. 2014; SER 2016).

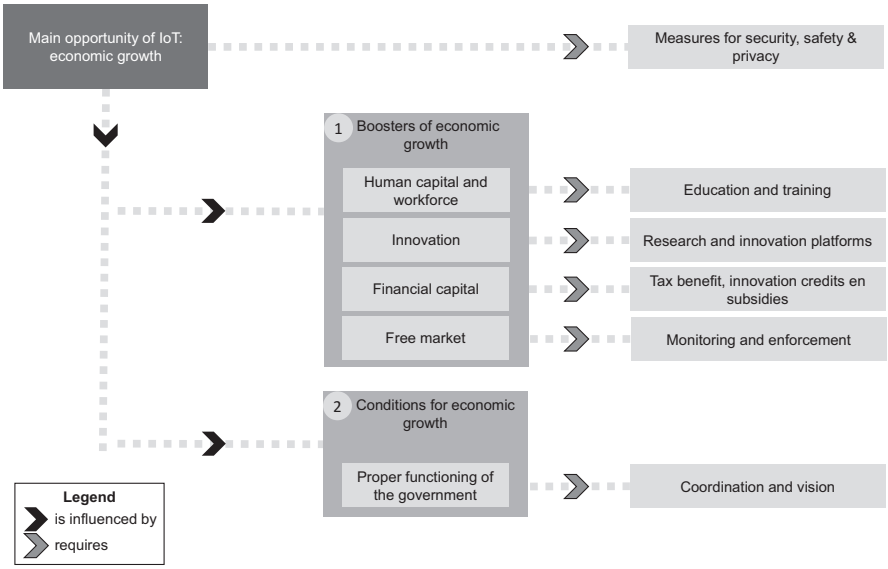


Fig. 1 Factors and measures that foster economic growth through the IoT

Government measures can ensure that the education system better nurtures the IT knowledge and skills needed. Possible solutions are to introduce specific courses that teach skills such as programming, or to incorporate IT skills in existing courses (GO-Science 2014). In addition, governments and organizations should also offer sufficient resources to (re)train the existing workforce.

Innovation

Innovation plays an important role in increasing the productivity of businesses and prosperity in countries. As discussed above, this is partly related to the availability of sufficient knowledge but also depends on the ability of businesses to apply this knowledge to product development and innovations. Businesses and countries that succeed in this challenge are able to stay competitive (CBS 2013).

Governments can support research into new IoT technologies and applications in order to promote economic growth. Universities, research institutes as well as companies with R&D departments can carry out such research. This support includes stimulating spin-offs based on research done at universities and co-development of new technologies by universities and businesses. It is also important that businesses get enough room to experiment and innovate. One possible solution is to implement a "regulatory sandbox," in which authorities work together with stakeholders to create safe spaces for exploring new applications (Vermeulen et al. 2016). Experiments done with self-driving cars in different countries are examples of this regulatory sandbox approach.

Capital

Capital involves both physical capital (buildings or machines) and financial capital. Availability of capital in a country determines, to a certain extent, whether businesses choose to invest in that country (CBS 2013). Governments can support businesses through different measures such as tax benefits, innovation credits, and subsidies.

Because of the importance of the IoT, governments should use financial incentives to stimulate IoT applications in those sectors that are important in their respective countries. In addition, startups should be given ample space to develop new ideas, for example through small grants that allow startups to develop a new IoT product. Governments could also stimulate the development of new IoT products by acting as an intermediary that connects startups with parties in traditional sectors.

Free Market

A free market mechanism is an important prerequisite for the development of the IoT and economic growth. It encourages companies to operate efficiently, create economic value, and share this value with customers (CBS 2013). Various policy instruments can be used to influence market forces, such as laws and regulations that determine the rules of a free market. These include, for example, labor laws and regulation that ensure a level playing field for domestic and foreign companies. Competition authorities are vital to safeguard a free market and to prevent unfair competition.

To ensure a free market in the wake of the IoT and its digital platforms, it is vital that competition authorities, both national and international, have sufficient resources to monitor and enforce applicable laws.

Proper Functioning of the Government

Government functioning influences the country's business climate (CBS 2013). Firstly, the government imposes rights and obligations on companies by implementing laws and regulations. Secondly, as a service provider, the government supports these rights and obligations by granting permits and subsidies, and levying taxes. Lastly, the government can also be a customer of certain products or services. For an optimal business climate, a certain predictability of a government's actions is favorable (CBS 2013). This reduces the risks for the businesses that want to invest. Research indicates that a smart government should take simultaneous actions to innovate technology, management, and policy, as governments need the normative basis in order to innovate (Eger and Maggipinto 2009; Gil-Garcia et al. 2016).

Developing a government vision for the IoT can help businesses to assess whether there is room to innovate and invest. This is especially important if these innovations challenge existing business models. Such developments could evoke

resistance within affected sectors and could call for stricter legislation. A clear government vision can help businesses to anticipate possible changes, and adjust investments accordingly. In this context, it is imperative for the government to take on a leading role as well as be a strategic customer of IoT innovations (GO-Science 2014).

To facilitate this vision new policies might be needed. Thierer (2015) states in this context that new technology should in principle be unrestricted, unless there are convincing arguments not to do so. Others have stated that if there is a lot of technological uncertainty, a technological neutral policy is preferred (Bijlsma et al. 2016). This means that if the adoption costs of new legislation are low for businesses, governments should facilitate experiments and wait with devising or imposing further legislations. Yet if the adoption costs are high, delaying new legislation is expensive (Bijlsma et al. 2016).

Previous studies suggest that there should be one body that is responsible for creating an IoT or technology vision and coordinating its implementation (GO-Science 2014; Kool et al. 2017). Experts that partook in this study, however, expressed worries that introducing a new body could be counterproductive and inefficient, as it creates yet another layer of government. Either way, our findings show that, given the wide range of measures discussed, there should be one party that coordinates and controls them to ensure their effectiveness.

Security, Safety, and Privacy

Figure 2 gives an overview of the *factors* (dark grey blocks) that can hinder the development and use of secure, safe, and privacy-sensitive IoT applications. These obstacles are (1) complexity of the IoT, (2) lack of knowledge and awareness, (3) lack of incentives, and (4) lack of monitoring and enforcement. For all these obstacles, the figure shows some *measures or solution directions* (light grey blocks) to reduce their impact. They are discussed below.

While in some cases it is difficult to take action, government policy could undoubtedly play a fundamental role in mitigating the risks. One could think of principles such as security and privacy by design, which requires that products and software be developed from the ground up to be secure. As a result, safety of both products and software is increased. The government should work closely with the industry to implement this approach on an international level, in order to safeguard the consumer from security threats.

Complexity

Complexity is one of the impeding factors in making IoT applications more secure, safe, and privacy-friendly. In this context, complexity stems from (1) the wide variety of IoT devices, (2) the processing of (big) data, and (3) the playing field. Firstly, the heterogeneity of IoT technology makes it challenging to intro-

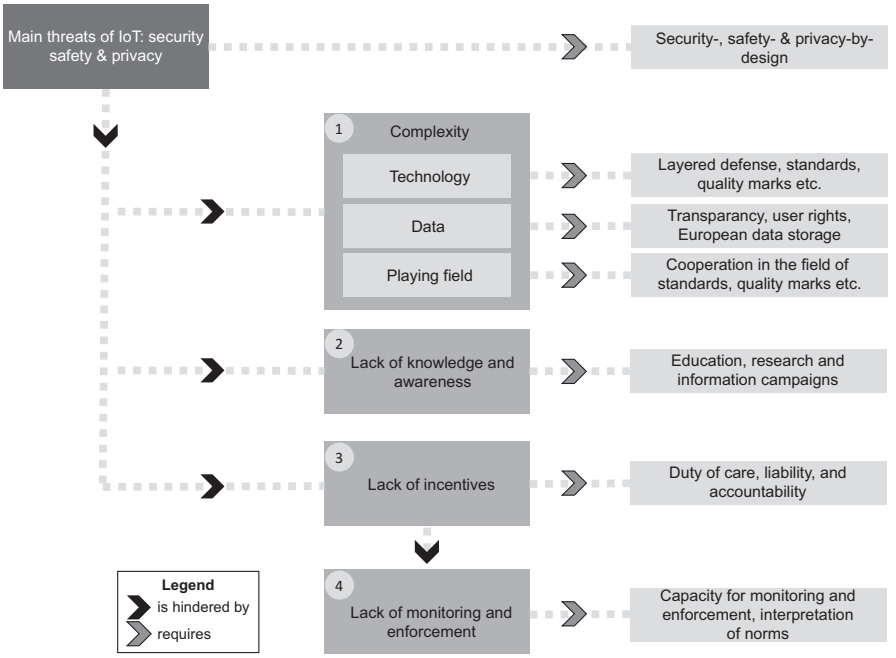


Fig. 2 Obstacles to developing secure, safe, and privacy-friendly applications, and solution directions to overcome them

duce general security measures. Secondly, the important role of data in IoT applications contributes to complexity because of the size and heterogeneity of the data, ambiguity about where they are stored, who has access to and makes use of them, and the legal interpretation of fundamental rights on data. Thirdly, due to the large amount of players on the IoT market, the (international) playing field is rather complex and lacks overview on who is responsible for what. This problem is worsened because governments involved have different rules and standards, as well as different interests.

The following governmental measures may contribute to coping with the complexity of the IoT. First of all, international conformity marks (i.e., CE marking) and standards can contribute to safety by harmonizing IoT technology. They help in determining which security and privacy requirements manufacturers of IoT products have to meet and make it easier to conform to them.

Secondly, transparency in data use can be increased by compelling companies to draft clear and understandable privacy policies. Agreements have been made in the EU's General Data Protection Regulation (GDPR)—article 12, obliging companies to present their policies in a concise, transparent, and understandable language to users. One way to provide users the right of removal of personal data is to integrate an on/off switch in devices, specifically for data transfer to third parties. Finally, localizing data storage can help confining data processing and usage. It should be noted that many of the measures discussed could be more effective when they are designed and implemented in an international context.

Lack of Knowledge and Awareness

Taking measures to mitigate security, safety, and privacy threats is also hampered by a lack of awareness and knowledge about (the risks around) the IoT and IT in general. This applies to the government, citizens, as well as businesses.

Education remains one of the most important duties of any government. Investing in education is, therefore, an important tool for increasing a safe Internet use and developing digital skills (CSR 2016b; Munnichs et al. 2017). In addition, knowledge institutions—such as universities—should emphasize security, safety, and privacy in their education related to developing and using IoT applications. Information campaigns on cybersecurity can also increase awareness and hence the digital resilience of citizens. Through research, knowledge about the current state of technology, cybersecurity and privacy can be acquired, maintained, and enhanced. Public–private partnerships can increase knowledge by monitoring and sharing information about current threats. This collaboration is already taking place; however, this should further be intensified to fully exploit the potential (CSR 2016b).

Lack of Incentives

Taking security, safety, and privacy measures is also impeded by a lack of incentives for users and businesses. Users are often unaware of security and privacy risks, and often, they do not even notice that their IoT devices are hacked (Kolias et al. 2017). For companies, there is an economic incentive to be first-to-market with a product, with or without adequate security features (Wolters and Verbruggen 2016). Moreover, once a device has been sold, their motivation to provide security updates is limited. Maintenance of a product requires time and money, and in most cases it does not yield benefits that outweigh its costs (Munnichs et al. 2017).

Though the lack of incentives applies to both users and manufacturers, in principle, users may assume that manufacturers sell sound products. Governments should therefore take measures that generate incentives for manufacturers to build secure, safe, and privacy-friendly products. One of these measures is to expand the duty of care legislation. Duty of care is an obligation "to take into account and possibly act in the interests of someone else" (Tjong Tjin Tai 2006: 376). The duty of care may also cover the security of IoT products. Liability on the basis of the damage caused by IoT products may also be an important incentive for companies and could serve as a basis for the duty of care.

In addition, the government can influence companies' incentives through their own purchasing policies. Hereby, the government can fulfill an example role as a launching customer. A new purchasing policy may also include the condition that only products and services that comply with certain cybersecurity standards are chosen, which may also serve as an encouragement to abide with certain standards and conformity marks.

Lack of Monitoring and Enforcement

The effectiveness of incentives is impeded by a lack of monitoring and enforcement. Without these, measures such as duty of care and liability have little effect. The same goes for conformity marks and standards, which are only effective with supervision and enforcement. An example of this can be found in the CE marking, which signifies that a product complies with current European requirements regarding safety, health and the environment. Nevertheless, various CE-marked products are withdrawn annually from the market as they pose a risk to users' health or safety (The Netherlands Court of Audit 2017). The Netherlands Court of Audit (2017: 7) indicates, among other things, that presently the resources and capacity are inadequate for effective supervision of the CE marking. This example shows that a label alone is not enough to ensure that a product meets certain requirements.

Further research and discussion on the duty of care for manufacturers of hardware and software are needed. Currently it is unclear, for instance, how duty of care and liability relate to the durability of products. Many products are only supported for a few years while they last many years. Therefore, it should also be considered whether companies should have obligations to provide support also after the expected product lifetimes.

Limitations

Although the research has reached its aims, we are aware of a number of limitations. Firstly, there is no clear definition of the Internet of Things concept. We have chosen to combine definitions, and in that way provide the reader with a comprehensive definition. Secondly, this research project encompasses various technologies and affects many application domains and stakeholders. Because of the large scope of this research, combined with a limited time within which the research had to be completed, it was decided to give a broad overview of the entire playing field. The relevant developments, players, and applications have been mapped out as much as possible. Such a broad focus causes the depth of the research to be limited. Lastly, this research did not aim to quantify the effect of different measures. The present research does describe the expected consequences of various actions, but does not discuss how strong the effects of different measures are. In a follow-up study, attempts could be made to measure the influence of the IoT on the named values (for example, to what extent does the IoT increase prosperity?). Subsequently, an attempt can be made to measure the extent to which certain proposed measures affect this. The interaction effects between different measures could also be taken into account.

Conclusion

In this chapter, we have shown that the IoT can contribute to a wide range of human values that correspond with public policy goals, such as well-being, sustainability, productivity, and prosperity. As such, the IoT can be used as a tool to achieve certain policy goals. At the same time, it also negatively affects certain values, such as security, safety, privacy, prosperity, well-being, equality, and autonomy. Therefore, the IoT may have a disruptive impact on society and cause physical, social, or economic damage. Because of this, both the positive and negative consequences should be taken into consideration when creating new public policy.

What is most worrying is that numerous examples and incidents show that IoT applications are currently poorly protected. This poses a serious threat to our security, safety, and privacy, but also hinders the ability to seize opportunities presented by the IoT. It is important that these risks are addressed in order to reduce and prevent damages as much as possible. To take advantage of the opportunities, it is also important to create a safe environment for new developments and innovation.

As manufacturers of IoT applications and infrastructures, companies are responsible for the creation of not only new and innovative but also secure and privacy-protective IoT applications. Currently this happens insufficiently due to the complexity of the IoT, a lack of knowledge, a lack of incentives, and a lack of monitoring and enforcement. We have shown that all these obstacles can and need to be addressed by government measures. Unfortunately, there is no one-size-fits-all solution for this problem. Instead, several interrelated measures are required, which are only effective if they are implemented as a whole. This requires a supported government vision, where one body is designated to control and coordinate a (new) IoT policy. Because the IoT is related to other technological developments and cybersecurity in a broader context, governments should adopt a coherent approach in which all these topics are covered.

References

Ackerman, S., & Thielman, S. (2016). *US intelligence chief: We might use the internet of things to spy on you*. Retrieved July 24, 2017, from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.

Amichai-Hamburger, Y. (2002). Internet and personality. *Computers in Human Behavior, 18*(1), 1–10.

Aoyama, T., Koike, M., Koshijima, I., & Hashimoto, Y. (2013). A unified framework for safety and security. *Safety and Security Engineering V, 134*, 67–77.

Arntz, M., Gregory, T., & Zierahn, U. (2016). *The risk of automation for jobs in OECD countries: A comparative analysis*. Paris: OECD Publishing. *OECD Social, Employment and Migration Working Papers,* 189.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Bawden, D., & Robinson, L. (2009). The dark side of information: Overload, anxiety and other paradoxes and pathologies. *Journal of Information Science, 35*(2), 180–191.

Beaudin, J. S., Intille, S. S., & Morris, M. E. (2006). To track or not to track: User reactions to concepts in longitudinal health monitoring. *Journal of Medical Internet Research, 8*(4), 1–22.

Bijlsma, M., Overvest, B., & Straathof, B. (2016). *Marktordening bij nieuwe ICT-toepassingen*. Den Haag: Centraal Planbureau.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications, 54*, 1–31.

Bos, J., & Munnichs, G. (2016). *Digitalisering van dieren*. Den Haag: Rathenau Instituut.

Bradley, J., Barbier, J., & Handler, D. (2013). *Embracing the Internet of everything to capture your share of $14.4 trillion*. San Jose: Cisco.

Castermans, J., Feijth, H., Verheij, M., Beekhuizen, J., & Wong-A-Tjong, S. (2014). *Internet of Things: Slimme en internet-verbonden producten en diensten*. Utrecht: Kamer van Koophandel.

CBS (Centraal Bureau voor de Statistiek). (2013). *Het Nederlandse ondernemings klimaat in cijfers 2013*. Den Haag: CBS.

Chang, R. (1997). *Incommensurability, incomparability, and practical reason*. Cambridge: Harvard University Press.

CLTC (Center for Long-term Cybersecurity). (2016). *Cybersecurity futures 2020*. Berkeley: University of California.

CPB & PBL. (2015). *Toekomstverkenning welvaart en leefomgeving: Achtergronddocument binnenlandse personenmobiliteit*. Den Haag: CPB/PBL.

CSR (Cybersecurity Raad). (2016a). *The opportunities and risks of the Internet of Things: Perspectives for action*. Den Haag: CSR.

CSR (Cybersecurity Raad). (2016b). *De economische en maatschappelijke noodzaak van meer Cybersecurity: Nederland digitaal droge voeten*. Den Haag: CSR.

Custers, B. H. M., Calders, T., Schermer, B., & Zarsky, T. Z. (2013). *Discrimination and privacy in the information society: Data mining and profiling in large databases studies in applied philosophy*. Heidelberg: Springer.

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Le Métayer, D., Tirtea, R., et al. (2014). Privacy and data protection by design—From policy to engineering. Technical report. https://doi.org/10.2824/38623.

Davies, R. (2015). The Internet of Things opportunities and challenges. Retrieved July 24, 2017, from https://www.europarl.europa.eu/RegData/etudes/BRIE/ 2015/557012/ EPRS_BRI(2015)557012_EN.pdf

Domingo, M. C. (2012). An overview of the Internet of Things for people with disabilities. *Journal of Network and Computer Applications, 35*(2), 584–596.

Ellen MacArthur Foundation. (2016). Intelligent assets: Unlocking the circular economy potential. Retrieved July 24, 2017, from https://www.ellenmacarthurfoundation.org/publications/ intelligent-assets

Eger, J. M., & Maggipinto, A. (2009). Technology as a tool of transformation: e-Cities and the rule of law. In A. D'Atri & D. Saccà (Eds.), *Information systems: People, organizations, institutions, and technologies*. Heidelberg: Physica-Verlag.

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on Internet of Things (IoT). *International Journal of Computer Applications, 113*(1), 1–7.

Fernandez, F., & Pallis, G. C. (2014). Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective. In *2014 EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth)* (pp. 263–266). New York: IEEE.

Flight, S. (2016). Politie en beeldtechnologie: Gebruik, opbrengsten en uitdagingen. *Justitiële Verkenningen, 42*(3), 68–93.

Floridi, L. (2015). *The onlife manifesto: Being human in a hyperconnected era*. Cham: Springer International Publishing.

Frenken, K. (2015). *Reflecties op de deeleconomie*. Retrieved July 24, 2017, from https://dspace.library.uu.nl/handle/1874/320399.

Friedman, B., Kahn, P. H., Jr., & Borning, A. (2013). Value sensitive design and information systems. In K. E. Himma & H. T. Tavani (Eds.), *Early engagement and new technologies: Opening up the laboratory* (pp. 55–95). Hoboken: John Wiley & Sons, Inc..

FTC. (2015). *Privacy & security in a connected world*. Washington: FTC.

Gartner. (2015). *What's new in Gartner's hype cycle for emerging technologies, 2015*. Retrieved July 24, 2017, from https://www.gartner.com/smarterwithgartner/whats-new-in-gartners-hype-cycle-for-emerging-technologies-2015

Gil-Garcia, J. R., Helbig, N., & Ojo, A. (2014). Being smart: Emerging technologies and innovation in the public sector. *Government Information Quarterly, 31*, I1–I8.

Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2016). Conceptualizing smartness in government: An integrative and multi-dimensional view. *Government Information Quarterly, 33*, 524–534.

Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulner-able and what we can do about it*. London: Transworld.

GO-Science (The Government Office for Science). (2014). *The Internet of Things: Making the most of the Second Digital Revolution*. London: GO-Science.

Gregory, J. (2015). *The Internet of Things: Revolutionizing the retail industry*. Retrieved July 24, 2017, from https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_14/Accenture-The-Internet-Of-Things.pdf

Healey, J., Pollard, N., & Woods, B. (2015). *The healthcare internet of things: Rewards and risks*. Washington: Atlantic Council.

Hildebrandt, M. (2008). Defining profiling: A new type of knowledge? In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen* (pp. 17–45). Dordrecht: Springer.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly, 32*(2015), 221–236.

Kaminski, M. E., & Witnov, S. (2015). The conforming effect: First amendment implications of surveillance, beyond chilling speech. *University of Richmond Law Review, 49*, 465–518.

Keymolen, E. (2014). A moral bubble: The influence of online personalization on moral repositioning. In J. de Mul (Ed.), *Plessner's philosophical anthropology: Perspectives and prospects* (pp. 387–406). Amsterdam: Amsterdam University Press.

Koebler, J. (2015). *Hackers killed a simulated human by turning off its pacemaker*. Retrieved July 24, 2017, from https://motherboard.vice.com/en_us/article/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84.

Kong, A., Beresford, S. A., & Alfano, C. M. (2012). Self-monitoring and eating-related behaviors are associated with 12-month weight loss in postmenopausal overweight-to-obese women. *Journal of the Academy of Nutrition and Dietetics, 112*(9), 1428–1435.

Kooiman, J., & Jentoft, S. (2009). Meta-governance: Values, norms and principles, and the making of hard choices. *Public Administration, 87*(4), 818–836.

Kool, L., Timmer, J., Royakkers, L., & Van Est, R. (2017). *Opwaarderen:- Borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut.

Krebs, B. (2016). *Who makes the IoT things under attack?* Retrieved July 24, 2017, from https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*(2), 122–136.

Lu, J. (2016). Will medical technology deskill doctors? *International Education Studies, 9*(7), 130–134.

Lund, D., MacGillivray, C., Turner, V., & Morales, M. (2014). *Worldwide and regional internet of things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand*. Framingham: International Data Corporation (IDC).

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. San Francisco: McKinsey Global Institute.

Mattord, W. (2014). *Principles of information security*. Delhi: Cengage India.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.

Moon, M. J. (2002). The evolution of e-government among municipalities: Rhetoric or reality? *Public Administration Review, 62*(4), 424–433.

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau Instituut.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge: Cambridge University Press.

Pandya, H. B., & Champaneria, T. A. (2015, January). Internet of things: Survey and case studies. In *2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO)* (pp. 1–6). New York: IEEE.

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review, 93*, 85–176.

Pereira, Â. G., Benessia, A., & Curvelo, P. (2013). *Agency in the Internet of Things*. Luxemburg: Publications Office of the European Union.

Roca, D., Nemirovsky, D., Nemirovsky, M., Milito, R., & Valero, M. (2016). Emergent behaviors in the Internet of Things: The ultimate ultra-large-scale System. *IEEE Micro, 36*(6), 36–44.

Roose, K. (2014). *The sharing economy isn't about trust, it's about desperation*. Retrieved July 24, 2017, from http://nymag.com/daily/intelligencer/2014/04/sharing-economy-is-about-desperation.htm

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: An overview: Understanding the issues and challenges of a more connected world*. Genève: Internet Society.

SER (Sociaal-Economische Raad). (2016). *Verkenning en werkagenda digitalisering: Mens en technologie: samen aan het werk*. Den Haag: SER.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.

Silver, E., Wallenstein, S., & Levy, A. (2012). Inward and outward: The role of patient self-monitoring and patient communities in IBD. *Inflammatory Bowel Diseases, 18*, 45–46.

Smit, W., Peters, S., Kemps, D., Vos, R., & Sterk, W. (2016). *Industrial Internet of Things: Noodzaak voor industrie, kans voor IT-sector*. Retrieved July 24, 2017, from https://insights.abnamro.nl/2016/02/industrial-internet-of-things

Song, A. M., Chuenpagdee, R., & Jentoft, S. (2013). Values, images, and principles: What they represent and how they may improve fisheries governance. *Marine Policy, 40*, 167–175.

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy, 42*(9), 1568–1580.

Stratix. (2015). *Internet of Things in the Netherlands: Applications, trends and potential impact on radio spectrum*. Stratix: Hilversum.

Sun, Y., Song, H., Jara, A. J., & Bie, R. (2016). Internet of things and big data analytics for smart and connected communities. *IEEE Access, 4*, 766–773.

Swan, M. (2013). The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data, 1*(2), 85–99.

The Netherlands Court of Audit. (2017). *Producten op de Europese markt: CE-markering ontrafeld*. The Hague: The Netherlands Court of Audit.

Thierer, A. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Richmond Journal of Law & Technology, 21*(2).

Tjong Tjin Tai, T. F. E. (2006). *Zorgplichten en zorgethiek*. Deventer: Wolters Kluwer.

Van den Berg, B., & Keymolen, E. (2013). Techniekfilosofie: Het medium is de maat. *Wijsgerig Perspectief, 53*(1), 8–17.

Van Est, R., & Kool, L. (2015). *Working on the robot society: Visions and insights from science concerning the relationship between technology and employment*. Den Haag: Rathenau Instituut.

Van Lakerveld, J. A., Broek, S. D., Buiskool, B. J., Grijpstra, D. H., Gussen, I., Tonis, I. C. M., & Zonneveld, C. A. J. M. (2014). *Arbeidsmarkt voor cybersecurity professionals*. Leiden: PLATO.

Verbeek, P. P. (2011). *De grens van de mens: Over techniek, ethiek en de menselijke natuur*. Rotterdam: Lemniscaat.

Vermeulen, E., Fenwick, M. Kaal, W. A. (2016). Regulation tomorrow: What happens when technology is faster than the law? *TILEC Discussion Paper No. 2016-024*.

Wang, Y. F., Lin, W. M., Zhang, T., & Ma, Y. Y. (2012). Research on application and security protection of internet of things in smart grid. In *IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012)*, 1–5.

Went, R., & Kremer, M. (2015). Hoe we robotisering de baas kunnen blijven: Inzetten op complementariteit. In *Wetenschappelijke Raad voor het Regeringsbeleid (WRR), De Robot de baas: De toekomst van werk in het tweede machinetijdperk* (pp. 23–46). Amsterdam: University Press.

Williams, C. (2016). *Thermostat ransomware*. Retrieved July 24, 2017, from https://www.theregister.co.uk/2016/08/08/smart_thermostat_ransomware.

Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The Internet of Things: A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261–274.

WEF (World Economic Forum). (2015). *Deep shift: Technology tipping points and societal impact*. Genève: WEF.

Weiser, M., & Brown, J. S. (1995). Designing calm technology. *PowerGrid Journal, 1*(1), 75–85. Retrieved May 17, 2018, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.9788&rep=rep1&type=pdf.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review, 64*(1), 15–27.

Wolters, P. T. J., & Verbruggen, P. W. J. (2016). De verplichting tot het bijwerken van onveilige software. *Weekblad voor Privaatrecht, Notariaat en Registratie, 7123*, 832–839.

WRR (Wetenschappelijke Raad voor het Regeringsbeleid). (2016). *Big Data in een vrije en veilige samenleving*. Retrieved July 24, 2017, from https://www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving

Wurman, R. S. (1989). *Information anxiety*. New York: DoubleDay.

Xu, T., Wendt, J. B., Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design* (pp. 417–423). New York: IEEE Press.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys & Tutorials, 15*(1), 5–20.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.

Zarsky, T. Z. (2014). Understanding discrimination in the scored society. *Washington Law Review, 89*, 1375–1412.

Zarsky, T. Z. (2016). The trouble with algorithmic decisions. An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology & Human Values, 41*(1), 118–132.

Zwenne, G. J. (2015). De onbestaanbare olifant: gedachten over Big Data en de Privacywet. *Tijdschrift voor Internetrecht, 4*, 142–147.

Ronald Pool is a senior legal advisor at ICTRecht and works as an in-house lawyer. Previously he worked as a researcher at the WODC, Dutch Ministry of Justice and Security. His research focused on cybercrime and issues concerning new technologies and law. He obtained his LLM in Law & ICT from the University of Groningen in 2014.

Jasper van Berkel received his BA in public administration and his LLM in law and technology from Tilburg University in 2011 and 2014. He is currently working as a researcher in the Crime, Law Enforcement and Sanctions Division at the Research and Documentation Centre (WODC). His research interests include cybercrime, cybersecurity, and the use of new technologies in the field of law enforcement. Previously he worked as a researcher in the Centre for Health Protection at the Dutch National Institute for Public Health and the Environment (RIVM). His research topics included e-medication, medical devices, and online patient empowerment.

Susan van den Braak is a senior researcher at the Statistical Data and Policy Analysis Division of the Research and Documentation Centre (WODC) of the Ministry of Security and Justice in the Netherlands. She holds a PhD in computer science from Utrecht University and an MSc in Artificial Intelligence from Radboud University Nijmegen. Her doctoral dissertation focused on argument mapping software for crime analysis. For the Ministry of Security and Justice she focusses on research in the field of AI and law, and e-government. She is currently working on data-centric information systems for policymakers which combine various large (judicial) databases. Her research interests include data science, big and open data, privacy, and cybersecurity.

Maaike Harbers is a professor of applied sciences in Artificial Intelligence & Society at Research Center Creating 010, and a senior lecturer at the Creative Media and Game Technologies program, both at Rotterdam University of Applied Sciences. Her work focuses on the intersection of artificial intelligence, ethics, and design. She studies how designers can create interactive, intelligent technology in a responsible way by accounting for the ethical and societal implications of their concepts during design time. She received a PhD in Artificial Intelligence from Utrecht University in 2011 and an MSc in artificial intelligence and an MA in Philosophy from the University of Groningen in 2006.

Mortaza S. Bargh obtained his PhD in Information Theory from Eindhoven University of Technology in 1999. Between 1999 and 2011 he carried out applied research and project management in the area of secure pervasive computing and ambient intelligence (topics such as system architecture, system security/privacy, and machine learning algorithms). Between 2012 and 2015 he was a part-time visiting Research Professor (i.e., Lector in Dutch) on cyber security and privacy at Rotterdam University of Applied Sciences (RUAS), and since 2013 he has been a scientific researcher at the research center WODC, Ministry of Justice and Security. Since December 2017 Mortaza has been appointed as Lector on Privacy and Cybersecurity Engineering at RAUS. His current research interests include privacy/security by deist engineering, privacy preserving data mining, machine learning, data publishing (e.g., in Open and Big Data settings), access and usage control, collaborative security, usable security, and risk management.

Methodologies for a Participatory Design of IoT to Deliver Sustainable Public Services in "Smart Cities"

Esther Ruiz Ben

Abstract Smart cities (Following Nam and Pardo (Conceptualising smart city with dimensions of technology, people and institutions, Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, pp. 282–291, 2011) I conceptualize smart cities based on three dimensions: technology, people, and community. Due to the use of ICT to fundamentally transform life and work in a city, these authors consider technology as a crucial dimension. In addition, the role of human infrastructure, human capital, and education, and the support of government and policies constitute crucial factors in a smart city too) seek to address public issues via digital connected solutions on the basis of a multi-stakeholder, municipally based partnership (http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf). This urban model includes using Internet of Things (IoT) facilities to deliver public services. However, the implementation of public service delivery and use through IoT in smart cities is frequently fragmented, hindering a sustainable urban development. Citizens remain unaware of multiple single tools developed without their participation. Security issues also prevent citizens from using IoT facilities in smart cities. The objective of this chapter is to explain the development of a participatory governance approach aiming to establish a sustainable development path for the design and implementation of public services for work and mobility delivered through IoT in smart cities. Departing from key issues extracted from existing research about public service delivery using IoT in smart cities, the approach adopts a socio-technical processual methodology combining several social research methods as well as visualization and game simulation techniques. The chapter concludes with a short discussion on the application of this participatory framework for the ongoing design and evaluation of sustainable public service delivery using IoT in smart cities.

Keywords Smart cities · Participatory urban design · IoT · Public service delivery · Sustainable cities · Data security

E. Ruiz Ben (✉)
Institute of Sociology, Technical University of Berlin, Berlin, Germany
e-mail: Esther.ruiz-ben@campus.tu-berlin.de

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_3

Introduction

The Internet of Things (IoT) basically understood as the Internet connection of people, process, data, and devices opens new opportunities and hides risks and uncertainties for the public sector. Opportunities, risks, and uncertainties need to be considered from multiple perspectives: policy leadership, services design, provision and regulation, local community development, environment protection, and citizens' lives. The design and implementation of IoT for public service delivery[1] involves organizational and professional changes such as the extension of leadership, accountability, and control through interoperability, requiring a comprehensive vision of the connected levels of policy (local communities, federal areas, and state) and of the integrated services involved at the different spaces. From the demand perspective, users need access, knowledge, and competence to use public services delivered through IoT. These requirements potentially increase digital divisions and create new boundaries between socioeconomic groups in urban settings.

Particularly in the context of smart cities where IoT is implemented on the basis of a multi-stakeholder municipally based partnership[2] to address public issues, opportunities, and risks specially related to transportation, safety, and environmental issues have been recently revealed affecting the differently involved actors (i.e. Pereira et al. 2017; Gascó 2016; Janssen et al. 2015). These include the benefits of transportation efficiency or information delivery (Ahvenniemi et al. 2017) as well as the citizens' uncertainties related to surveillance (Firmino et al. 2013) that can lead to mistrusting public service delivery through IoT. Public administrations confront a difficult dilemma in the design of efficient and effective IoT systems for safety purposes or for disasters responses that at the same time protect citizens' privacy in urban spaces. In addition to the citizens' mistrust of IoT in smart cities, citizens frequently ignore the existence of public services delivered through IoT. Smart and sustainable city concepts are rarely integrated in a common vision for urban development including citizens' perspectives (Robinson and Cole 2015; Turcu 2013).

[1] I refer to public service delivery as the provision of outputs such as welfare benefits, roads, and schools. As Alford and O'Flynn (2012: 8) explain, service delivery is a subset of a larger body of activities described in the literature as "implementation" or, in other words, putting police into effect.

[2] I refer to stakeholders in the context of smart cities as persons who are involved with a public or private organization that develops products or services for smart cities and therefore has responsibilities towards the organization and the smart city and an interest in their success. Actors are not necessarily attached to a particular organization. The term actor generally refers to persons, organizations (Geser 1990), or entities (Latour 1999) to which actions and action outcomes are attributed. Actor-network theory considers interacting human and machines as networks acting as autonomous actors (Latour 1999). This might be the case of IoT that entails technologies and users collectively acting in smart cities.

For an explanation about multi-stakeholders municipally based partnership see http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf

These concepts normally neglect users' participation in "smartification[3]" processes. The implementation of "smart" urban concepts frequently involves policy, organization, and management-related risks (Nam and Pardo 2011).

A participatory approach (Gabrys 2014) that includes multiple actors (public services deliverers, IoT companies, local communities, users, local, federal, and state actors) in the design and implementation of IoT in urban spaces could contribute to prevent these risks and reduce the uncertainties related to the sustainability of smart cities' projects. In the context of smart cities, some scholars suggest to use technologies to enabling sustainable development of cities (Bifulco et al. 2016). This means to think on technologies as enablers of sustainability, including environmental, social, and economic aspects in urban design, instead of considering technologies as an end in themselves (Marsal-Llacuna and Segal 2016; Ahvenniemi et al. 2017). The objective of this chapter is to explain the development of a participatory governance approach aiming to establish a sustainable development path for the design and implementation of public services delivered through IoT in smart cities (Löw 2012). To concretize the scope of the chapter, the approach concentrates on mobility and work in smart cities. This methodology approach combines several methods in different analytical phases and goes beyond existing simulation tools of smart cities mainly focused on functional issues (Zambom Santana et al. 2016; Zanella et al. 2014). The several methods proposed (qualitative and quantitative methods including visualizations and simulations (Ruiz Ben 2017; Bell et al. 2016)) are conceived to firstly identify the different actors involved in the design, implementation, and maintenance of IoT tools for public service delivery related to work and mobility in smart cities and understand their perspectives. These methods will further help to understand how users adopt these tools in their everyday lives. In a second step, the visualized adoption practices are used for the design of participatory governance practices and tools. These are simulation games with citizens and multiple stakeholders in concrete smart cities scenarios targeted at integrating some key features of smart and sustainable cities such as smart sustainable mobility based on Bell et al. (2016) ideas.

The chapter is structured in four parts. In the first part I explain existing concepts to use IoT for public service delivery and show some implementation examples in smart cities (London as an example of a smart city with experience in the organization of the Olympic Games and Chicago as well as Vienna as examples of cities with positive experiences in the implementation of IoT in smart cities). In the second part I discuss the research outcomes about the socioeconomic and environmental impact

[3] I conceptualize smartification in this chapter as the process through which multiple devices, infrastructures, and people are interconnected using digital technologies. The main characteristic of smartification in urban settings is the interconnectivity between devices, infrastructures and people in a particular urban space. I use the term "smartized" for those devices and infrastructures in smart cities that are already interconnected through digital technologies.

I distinguish between digitization as the process of moving information from analogue to digital formats, which can be analyzed using computers and digitalization as process by which digital computer methods and technologies are applied in social, cultural, economic, and industrial domains.

of public service delivery using IoT in smart cities. I identify key aspects of research and move to overview participatory approaches in the design of smart cities in order to extract basic ideas to conceptualize the participatory methodology framework that I elaborate in the third part of the chapter. The chapter concludes with a discussion about possible implementation scenarios and the benefits and risks of using the proposed methodological framework for the participatory development of public service delivery using IoT in the context of smart cities.

Conceptual Applications of IoT for Public Service Delivery: Some Implementation Examples in Smart Cities

The Internet of Things (IoT) constitutes a communication paradigm intending to enable and develop the communication between devices used in everyday life equipping them with microcontrollers, transceivers, protocol stacks, and so on in order to be used through the Internet. Through the IoT users can access and interact with many different devices such as vehicles, home appliances, and monitoring sensors. While at the same time they generate data about their everyday habits. These data can also be easily compiled by companies and public organizations (Zanella et al. 2014) which brings uncertainties, risks, and opportunities for the differently involved stakeholders (Jing et al. 2016; Kushner 2013; Popescu and Radu 2016). From the technological point of view the IoT is a broadband network consisting of three layers (the perception layer, the network layer, and the application layer). In the perception layer the Internet-enabled devices perceive and exchange information with each other. In the network layer the "perceived" information is forwarded to the application layer which is the place where the information is received and processed (Talari et al. 2017). The perception and the network layers are managed by the city, whereas service providers develop and run the apps and digital devices providing the interface to the users (FTTH Council of Europe 2015). Many cities have already implemented networked sensor environments often organized as public private partnerships between city governments and multinational companies as well as other design and engineering firms.

The potential of this communication paradigm for developing smart cities[4] is as enormous as the uncertain challenges it brings for suppliers and users. Some authors have criticized the lack of clarity in the concept of smart cities as well as its overenthusiastic and rhetorical character (Hollands 2008) and frequently ignoring the data privacy, data protection, and data security risks related to the implementation of the IoT communication paradigm (Kitchin 2016). These include the lack of opportunity for giving meaningful consent to process personal data, the degree to which different actors collect private data from inevitable public interactions, the repurposing of

[4] For an overview of the multiple definitions and ideas associated with the term "smart cities" see Nam and Pardo (2011).

"big data" drawn from IoT in smart cities as well as the storage of that data in the cloud (Edwards 2016).

Despite these multiple uncertainties and risks, IoT has been recently applied in many different areas including the provision of public services in smart cities. Surveillance systems including CCTV, public place monitoring, people and object tracking, or traffic police are some examples for security applications, while air quality and noise pollution monitoring, energy efficiency monitoring, or renewable energy usage are examples for environmental monitoring in smart cities. In the area of traffic management, IoT has been applied for example for travel scheduling or traffic jam reduction but also for smart parking and traffic monitoring. Healthcare, weather, and water system monitoring are other samples of the use of IoT in smart cities for public service delivery (Talari et al. 2017).

Many cities began to apply the IoT paradigm for delivering public services all over the world during the last decade. This is, for example, the case of London where the government initiated in 2013 a strategic plan for the making of the city smart, which originated with the purpose of managing the city traffic for the occasion of Olympic Games in 2012. The smart London Plan created by a board[5] of academics, businesses and entrepreneurs comprised seven topics: (1) placing Londoners at the core of innovation, (2) providing access to open data, (3) leveraging London's research technology and creative talent, (4) facilitating networking among and with other smart city stakeholders, (5) enabling "smarter" infrastructure development and management, (6) providing more effective and integrated City Hall services, and (7) offering a "smarter" London experience for all.[6] The plan envisioned three main priorities: engaging citizens, enabling good growth and working with business. To engage citizens the program experimented with tools such as "talk London focus groups" or "micro-volunteering programme" to get feedback for strategy and delivery of public services with IoT. Another way of supporting the participation in the development of London as smart city has been the program for increasing Londoners' digital skills (Greater London Authority 2016).

In Chicago, a project supported by the University of Chicago used digital tools for sharing information between residents, organizations, police, and communities to overcome violent crimes. In order to build trust several data collected by the police, users and agencies have been made available for a smart phone application using a mapping interface and GPS (Talari et al. 2017). Moreover, five demonstration sites have been established in the city to show how digitalization works in an urban context, and a network of 250 free-of-charge computer labs and digital skills training centers ("Connect Chicago") has been launched to engage the citizens in this evolving smart urban setting (Zelt 2017).

[5] https://www.london.gov.uk/what-we-do/business-and-economy/science-and-technology/smart-london/smart-london-board

[6] http://www.urenio.org/2015/01/19/smart-city-strategy-london-uk/

These examples show the widespread of the IoT paradigm for delivering public services in smart urban settings all over the world. However, a recent evaluation of 87 smart cities shows that though the idea of using digital tools and infrastructures for delivering public services in urban settings exists since years in numerous cities as a widely acknowledged positive urban development concept, the implementation of this idea seems to be very fragmented with lack of concepts addressing the whole population and their diverse ways of living. The research confirms the lack of holistic design (Lee et al. 2013) and consistent definition of smart cities (Madner et al. 2012) and reveals a "silo mentality" among the municipal administrators involved in taking their approach to digitalization, resulting in multiple disconnected projects. Those cities (Vienna, Amsterdam, and Seoul) where a central coordination exists show more positive results in the implementation of smart urban strategies. The main focuses of the public services delivered in the cities included in the research are government administration, energy, and environment as well as mobility. In terms of governmental issues, Chicago, Cape Town, and Stockholm are the best scoring cities among those covered by the research (Zelt 2017).

For example, in Vienna, the city with the best scores in this research, public services are being comprehensively shifted online. Moreover, in collaboration with schools, universities, and community colleges, Wi-Fi facilities are being expanded throughout the city. The framework for developing Vienna as a smart city bases on three key objectives: resource preservation, improving quality of life (including the provision of low-cost and resource-conserving mobility using IoT), and development in innovations. Particularly important for the successful implementation of the smart city framework in Vienna has been its participatory approach. As part of its governance strategy, this approach includes the "strengthening of the participation possibilities of citizens and experts" as a priority. Some examples of the implementation practice of this priority are, "Large-scale rollout of open government as a principle and driver of innovation. Regular Smart City Wien stakeholder forums. Development of formats that transport Smart City Wien issues to kindergartens, schools and other educational establishments: a major initiative makes topics like energy efficiency, low-impact mobility, virtual worlds or coexistence in a city without poverty part of the syllabus and enables children and young people to build their own smart Vienna: '100,000 kids design their very own smart city'." (Vienna City Administration 2014: 89). In the next section I concentrate on the participatory approaches for the design and implementation of smart cities discussed in the literature (information systems, administration science and urban studies). The extracted ideas from this literature overview will serve to develop the methodological framework explained in the third section of the chapter.

Overview of Participatory Approaches in the Design of Smart Cities: Basic Ideas to Conceptualize the Participatory Methodology Framework

Citizens do not normally participate in the early phases of the design of smart cities. They are included as users once the "smartification" processes are deployed following technological priorities. This leads to a frequent mutual unawareness between suppliers and citizens about public services implementation and usage with IoT. Unawareness and uncertainty about usage implications of public services delivered through IoT in urban settings lead to data security problems in the frequently fragmented IoT projects that coexist in smart cities. I argue that the lack of usage and the security problems emerging in the fragmented development of public service delivery using IoT in smart cities is not just a technological challenge or a question of "disciplining" the so commonly called in the IS literature "human factors." As Kitchin (2016) argues, the solution for neutralizing the negative effects of creating smart cities needs a multiple approach that includes policy, regulatory, and legally aspects as well as governance and management. This means to apply revised fair information practice principles as well as privacy and security by design, education, and training (Kitchin 2016) for building awareness about data security and privacy issues through early citizens' participation in the design of IoT in smart cities.

In order to develop a participation framework for the making of smart cities, it is useful to take into account the numerous experiences in the implementation of IoT concepts for the development of these urban settings. These experiences bring some key outcomes about risks and opportunities of IoT deployment in smart cities. In this section I focus on participatory approaches in the design of smart cities to extract key aspects to conceptualize the participatory methodology framework that I elaborate in the third part of the chapter.

Participatory research has been developed and used in several areas of production engaging people at the beginning of the product cycle when the design is not even initialized. This allows to include the ideas of diverse groups of citizens that can later be discussed. Early engagement of people in production design also frequently reveals different constraints in the realization of the product due to existing regulations, market features, personal values, local culture, or community habits, among others (Sanders and Stappers 2014).

Emphasizing the important role of citizens in urban design planning as well as their rights to decide about the cities they want to inhabit, several actors (architects, urban planners, interaction design researchers, etc.) have used participatory design approaches (Foth et al. 2015) in the context of smart cities. These approaches are applied at different phases of smart cities' planning and development and oppose the idea of considering citizens in smart cities as mere users of innovative digital technologies. They aim at applying digital technologies to connect the communities living in smart cities with their urban environment. Some examples of this participatory design approach for smart cities are digital place-making (Fredericks et al. 2016; Tomitsch and Haeusler 2015), urban interaction design (Brynskov et al. 2014),

urban informatics (Foth et al. 2011), and urban human–computer interaction (Fischer and Hornecker 2012).

Another form of participatory approach consists in the engagement of citizens in particular topics concerning different phases of the smartification of cities. The direct engagement of citizens in urban design topics using SMS and Twitter to respond to particular community issues has been investigated by Schroeter and Foth (2009). Similarly, researchers have used other digital devices to engage citizens in urban topics; for example, Boring et al. (2011) used media façades for collaborative interactions in public spaces, Hoggenmüller and Wiethoff (2014) applied public displays to engage with people in urban spaces, including through hand gestures, and Memarovic et al. (2011) deployed interactive touchscreens in public urban areas.

Another participatory approach seeks to engage citizens in voting for urban topics. This has been applied by Hespanhol et al. (2015) using two different "Vote As You Go" input interfaces in conjunction with an urban screen in a public square. One application consisted of a tablet with survey running on it and being live projected to an urban screen. The other application had an interactive body movement interface which was also shown live on the screen. The interfaces served to citizens' participation in urban issues attracting persons passing by and at the same time showing the running results of the public survey. Taylor et al. (2012) used digital voting devices in urban areas seeking to attract the citizens' participation in urban questions as well. Similarly to Hespanhol and Tomitsch (2015) experience, Taylor et al. (2012) digital application displayed the accumulated results of the citizens' answers. More recently, other scholars have further developed these digital interactive techniques for the participation of citizens in urban issues. Fredericks et al. (2015) conducted several interventions with digital interfaces and pop-ups in a live public view screen aiming to engage passers-by from diverse demographic backgrounds. They combined the presentation of the survey results with static pictures highlighting how interactive digital methods can effectively serve to improve the direct community participation of diverse citizens in urban issues. Other examples of the further development of participatory digital technologies for urban design are the "InstaBooth" applied by Caldwell and Foth (2017) or Fredericks et al. (2017) field studies using several digital and analog techniques for citizens' submission of opinions about city making initiatives.

In sum, these approaches aim to engage citizens in given urban issues using digital technologies once the technologies and the uses are designed and implemented. However, how citizens imagine the cities they inhabit as "smart" environments or what particular aspects they would like to be digitalized or not and why are neglected aspects. This can lead to unawareness and indifference of public service delivery through IoT from potential users or even misuse or abuse (e.g., in cases of data security and protection). Key aspects that can be extracted from previous research are (a) the lack of citizens' participation in the design of smart cities; (b) the lack of mutual awareness between different implementation choices of IoT for public service delivery in smart cities.

Other researchers have applied participatory approaches already used in other disciplines (see for example Chambers 1995; Fraser et al. 2006; Buscher et al. 2002;

Cinderby 2010) to include people from the early phases of urban design attempting to overcome these risks.

Some recent research has used this approach for encouraging a diverse population in the early phases of the making of smart cities departing from the idea that using digital technologies can exclude many citizens who do not use these technologies for various reasons. For example, the research of Bell et al. (2016) adopts a co-design approach including citizens as participants in the design practice as well as design experts. The researchers applied their participatory approach (MMM: Making Metrics Meaningful) over a 5-month period with self-selected transport users to gain insights from the general public into new ways of designing public transportation for smart cities. The methodology includes picture creation and programmatically specific musical "signatures" as well as group discussions to elicit citizens' concerns, needs and ideas about transportation design in their smart becoming city. Based on previous experiences in the context of metrics measures for local sustainability (Bell et al. 2016), the project included the Rich Picture method consisting of a device for collecting thoughts from groups of around 5–10 stakeholders. The participants are provided with colored marker pens and a large poster sheet of paper where they can together express their thoughts about a particular issue through drawings and writings. The researchers conduct a content analysis of the poster called "eductive interpretation content analysis" (EICA) (see Bell et al. 2016). In this analysis the researchers firstly focus on specific themes observed during the drawing session as well as in the poster itself such as the stakeholders' style, the facial and body language, the group's interaction, the usage of the surrounding spaces or the dominant icons used. The researchers further collect the themes that the stakeholders use for the description of their picture. Finally, the research team eventually in collaboration with the stakeholders summarizes their reflections about all previous steps. The results of this research phase were used in a second workshop to reflect with the stakeholders and encourage them to participate in a further design of an innovative technology for the smart city they inhabit. Following Baranauskas's (2014) socially aware computing approach, stakeholders from diverse backgrounds were included in the technology design through the Rich Picture and EICA methods as well as through a musical signature for each participating group. In a second workshop dedicated to the technology design, the interested participants were younger due to their previous technology experience. They were asked about the design and usage of particular new technologies in their daily lives. Departing from that, the participants should design the user interface of the imagined technologies as well as define which data they would like to include for them. This research is limited to transportation issues in smart cities. However, the methodology used departing from the idea of including the citizens in the making of smart cities can be very helpful for the development of participatory approaches in sustainable public service delivery in smart cities. For the methodology proposed in this chapter, citizens could also be asked about the use of IoT for the transportation information to access their workplaces.

Another approach for engaging citizens in the making of smart cities consists in the application of the so-called serious games. In contrast to entertaining games,

serious games are more complex containing not only a story, art, and software development but also pedagogical strategies that discern learning theory, teaching and learning approaches, assessment, and feedback (Zyda 2005; Cornillie et al. 2012; Raybourn 2014). Serious games have been applied in numerous fields including military, education, well-being, advertisement, cultural heritage, interpersonal communication, and health (Laamarti et al. 2014). Due to the rapid developments in smart cities implementation, scholars have used serious games for simulating several aspects of smart cities. For example, Urban Data Game (UDG) aims to motivate the learning of data skills for big, live, data sets. This game bases on principles of narrative, game-based learning, inquiry, collaborative learning, and challenge. The UDG includes a so-called Eco-Puzzle and an Appathon. The Eco-Puzzle confronts the participants with finding out what has happened in a recent disaster occurred in a urban setting. The participants must do this in the shortest time and present a compelling justification, backed by data visualization and analysis querying the data sets and narrowing down the time frame for an event. Another example connected to the application of serious games for awareness about smart cities services is the recent development of a Datascape (Wolff et al. 2017) with the goal of exploring the possible benefits of a tangible map-based interface to help users to gain a better sense of open data. The designers of this game depart from the evidence that citizens frequently do not use available open data (Janssen et al. 2012).

In sum, previous research shows that the implementation of IoT for delivering public services involves socioeconomic as well as environmental risks. Some of these are not exclusive to public service delivery. Key aspects that can be extracted from previous research are (a) the lack of socio-technical holistic implementation and governance approaches including environmental aspects and the inclusion of diverse stakeholders (including public servants) from the early phases of public services design using IoT. (b) Unawareness and uncertainties about data security risks of using public services delivered by IoT.

Security issues are for example common to every use of IoT in smart cities. The main concerns about data security in smart city technologies are the capture, storage, sharing and misuse of data produced by these technologies. Digital technologies in smart cities can capture personally identifiable information as well as household level data about citizens—characteristics, location and movements, activities—link these data creating recombined data, and use them to produce profiles of citizens and places to take decisions about them. Moreover, the security of smart cities technologies as well as the data they generate is vulnerable to hacking and theft which raises questions about the uncertainties and implications of a data breach for citizens. However, citizens in smart citizens are frequently unaware about the risks of the smart devices they use or about the security implications of certain devices usages habits. For example, when devices are not adequately configured, proper authentication is not used or when terms and conditions about data collection by applications is ignored. Smart cities users frequently do not properly protect stored sensitive data and receive malware through spam emails or social media. In addition, citizens are often not aware about the data collection, processing, storage

and transmission of personal data sent to smart city managers (Popescu and Radu 2016).

The next section focuses on the explanation of a proposed participatory methodology framework aiming to include diverse stakeholders groups in the design and development of these services in the making of smart cities.

Socio-Technical Participatory Methodology Framework

The review of the literature about public service delivery using IoT in smart cities has revealed the following key issues:

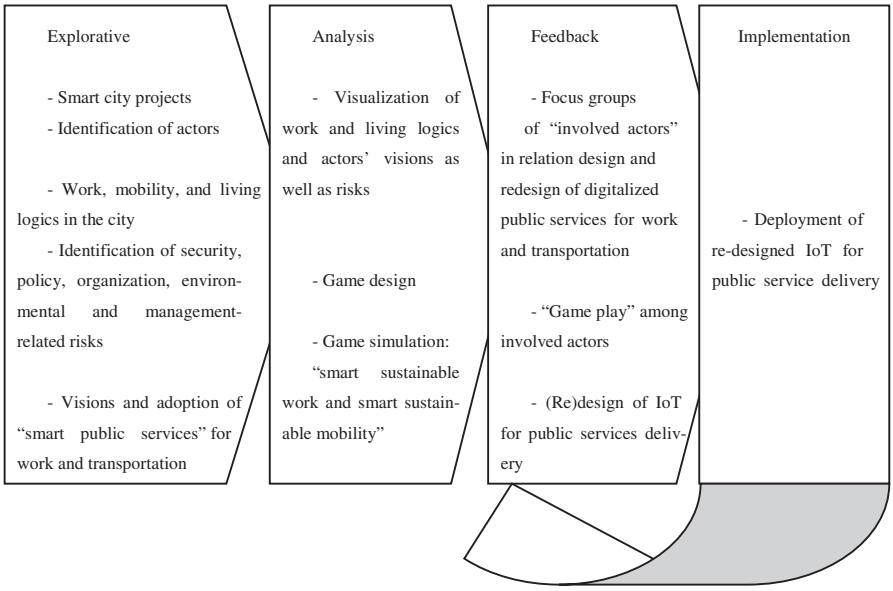
(a) The lack of socio-technical holistic implementation and governance approaches including environmental aspects and the inclusion of diverse stakeholders (including public servants) from the early phases of public services design using IoT).
(b) Unawareness and uncertainties about data security risks of using public services delivered by IoT.
(c) The lack of citizens' participation in the design of IoT for smart cities.
(d) The lack of mutual awareness between different implementation choices of IoT for public service delivery in smart cities.

Departing from the question: *What governance practices can enable a sustainable development and implementation of public service design and delivery for work and mobility using IoT in urban environments?* I build a participatory approach to empirically extract tools for establishing a participatory design and governance framework for the development of public services using IoT in smart cities. In this section I focus on the design ideas for this approach.

Based on the existing participatory methodologies commented above as well as from the main socioeconomic and technological aspects learnt from the explained previous research, I suggest to apply a processual approach combining qualitative and quantitative social research methods. The aim of this methodology will be first to identify the appropriate stakeholders involved in the delivery of public services for work and mobility using IoT to further understand the living logics of the urban settings being "smartized" (social, economic, and environmental) focusing on work and mobility aspects as well as in security risks (see explorative phase in Table 1). In a second step the methodology uses the gained understandings about the particular living logics of the smartized public services for work and mobility to develop visualizing scenarios and simulating sustainable working and mobility games (see analytical methodological phase in Table 1). This constitutes an ongoing participatory process involving citizens from the early phases of urban and technological design to avoiding fragmental governance revealed in previous research about the implementation of smart cities.

For the operationalization of sustainable governance I use Ahvenniemi et al.'s (2017) indicator system that includes economic, social, and environmental aspects

Table 1 Participatory approach: processual socio-technical methodology



of adoption of public services delivered through IoT in particular urban settings. I adapt this indicator system to the concrete socio-technical analysis of the logics of work and mobility using IoT for public service delivery in a particular smart city. For example, Shin et al. (2012) comment that IoT systems have significant socio-technical implications.[7] They "may interfere with established work practices, undermine productivity and individuals' satisfaction, and have an unforeseen impact on relations of power and control." As the authors further point out, these IoT interferences of institutionalized work practices are neglected in the research about IoT. These implications of IoT for work in the context of smart cities are one focus of the framework proposed in this chapter. This means to investigate how IoT technologies used for delivering public services in relation to work (e.g., IoT facilities for working and communicating in public spaces) affects the working and living logics of citizens in particular smart cities. These logics include citizens' mobility

[7] The term "socio-technical" refers to Bijker's (1995) idea that technology should be analyzed in relation to the social context where it emerges and society in relation to technological systems. Both technology and society conform to a socio-technical ensemble. In this ensemble different groups with their own interests struggle to fix a meaning for a particular technology. Once the disputes about the particular technology are settled, the meaning of the technology is stabilized and "forms part of an enduring network of practices, theories and social institutions" that are difficult to change (Bijker 2001: 28). Related to the meaning of technology created in "socio-technical ensembles," "boundary objects" are "objects that both inhabit several communities of practice and satisfy the informational requirements of each of them" (Bowker and Star 1999: 297). These "boundary objects" can serve to identify the stakeholders producing the meanings of a particular technology (Fischer 2007).

for working in the context of a particular smart city which constitutes the second focus of the proposed framework. Applying the ideas of Martina Löw (2008) I understand the living logics of a smart city as their intrinsic urban character that pre-structures particular development opportunities and spatial arrangements for deploying IoT. Thus, for the proposed framework, the particular living logics of work and mobility of the concrete smart city should be analyzed in relation to the institutionalized meanings and practices of use of IoT.

For example, if we aimed to analyze the governance practices that enable a sustainable development and implementation of public service design and delivery for work and mobility using IoT in London, as example of a smart city, we would begin finding out which projects do already exist or are planned and who is involved in their design and implementation. This explorative analysis will serve to identify the stakeholders of public service delivery for work and mobility using IoT. To ensure that the identified stakeholders are appropriate for the analysis, it would be proofed that they are directly involved with the design, implementation, and further development of IoT for the specific area of public services for work and mobility in the selected city (e.g., in London). We would also analyze how the public services offered with IoT facilities are used in the different neighborhoods of the city. This would enrich the already existing approaches used for analyzing the development of smart cities adding an understanding of the particular logics of public service delivery for work and mobility using IoT. This specific topic has not been analyzed yet.

We would further need to build indicators about how the already implemented IoT technologies used for public service delivery, socially, economically, and environmentally affect the particular working and mobility logics of the city. These indicators would be built during the explorative phase of the proposed participatory approach.

Examples of social, economic, and environmental indicators related to work and mobility using IoT—adapting Ahvenniemi et al.'s 2017: 239) analysis—would be "perception of getting a new job" or "foreign language skills." Other possible indicators would be "use of public spaces for tele-working"; "use of public transport information for getting to the workplace"; "use of IoT infrastructures for co-working in public places." Another indicator in relation to mobility could be the frequency of travelling beyond the own neighborhood for working in public spaces. Also related to this, it could be analyzed whether this mobility leads to a more integrated city avoiding spatial fragmentation and social segregation. An indicator for this would be the frequency of face to face social relations maintained due to work in public spaces using IoT in different neighborhoods. These indicators could also enrich Ahvenniemi et al.'s (2017) approach.

Examples of indicators for data security risks of using public services delivered by IoT would be "protection of stored sensitive data in public workplaces," "data collection, processing, storage and transmission of personal data sent to smart cities' managers" (Popescu and Radu 2016).

Later in the analytical phase these indicators would be used for visualizing scenarios and for the design of a simulation game. This game would include data security aspects and would be tested by differently involved actors during the "feedback"

phase. The introduction of security aspects as a part of the participatory approach could also enrich the existing participatory approaches that neglect data security issues.

The outputs from the first approximation to the particular logics of the public services delivered through IoT in the specific smart city (e.g., London), (identifying the different involved actors, their motives and design as well as use/nonuse of public services delivered through IoT and the risks involved) will serve as a basis to visualize particular smart cities logics centered at particular aspects of urban lives. These outputs will also serve to design a game (based on Datascape ideas (Wolff et al. 2017)) for encouraging all involved actors in the smartization of urban settings to participate in its development and give feedback to the actors in the technological design and implementation of the IoT used for public service delivery.

For the visualization of work and living logics the approach uses available data about mobility from smart payment systems for urban transport networks (Avoine et al. 2014) or real-time data from Google maps, Apple maps, Bing maps, and so on. Moreover, the "visions" and risks related to the use of IoT for public service delivery and use collected through online surveys are visualized and used for discussing them in focus groups and for the design of a game about work and living in a smart city. This allows to include not only citizens but also public servants (van Waart et al. 2016) in the early design of IoT use for public service delivery and use. At the same time, visualization of the logics of the urban settings can encourage the citizens to use the available public services delivered through IoT. This is for example the case with transportation apps such as KickMap[8] (Mitchell et al. 2015). To support the visualization of living logics and the game design, in the analytical phase the method applied by Bell et al. (2016) is used in this approach. This method developed as a means to engage communities in the design of local sustainable measures consists of collecting data on selected indicators from diverse local communities using the so-called "rich pictures." Rich pictures are diagrams produced with few rules than the use of as few words as possible. The diagrams are produced in groups on a large poster sheet of paper with colored marker pens. The diagrams are interpreted following a content analysis system (Bell et al. 2016). In the approach presented in this chapter, this method is used during the analytical phase for understanding the sustainability of public services delivered and use with IoT and for designing a simulation game.

Moreover, the extracted outputs from the analytical phase are used in the feedback phase to discuss in focus groups design scenarios of public service delivery using IoT. During this feedback phase the simulation game tested in the previous analytical phase is "played" by diverse stakeholders who give feedback about the design and possible redesign of public services using IoT. In the last phase the redesigned tools are implemented, and the feedback phase commences again using the proofed analytical tools.

[8] http://www.kickmap.com/

In sum, the methodology proposed and still to be tested, includes four phases in which different methods are combined to analyze first the ideas and expectations of citizens/users about public service delivery using IoT, the identification of involved actors in design and implementation of the public services and the security, policy, organization, environmental, and management-related risks of adoption forms. Second, it helps to develop participatory governance practices and tools to create a mutual trust between involved stakeholders and to manage the risks and uncertainties related to the delivery of public services with IoT in smart cities commented above (security, unawareness, etc.).

Discussion and Conclusions: Possible Implementation Scenarios and the Benefits and Risks of Applying the Proposed Methodological Framework for the Participatory Development of Public Service Delivery Using IoT in the Context of Smart Cities

In this chapter I have explained how to develop a participatory approach for design of IoT to deliver sustainable public services in "smart cities." Though the idea of using IoT for delivering public services in urban settings is widely acknowledged as a positive urban development concept, its implementation is frequently fragmented among many unconnected projects lacking sustainable concepts addressing the whole population and their diverse ways of living. A mutual unawareness between the different stakeholders, including the users, is one of the implications of this, but also mistrust and uncertainties about possible data protection and security risks. Several scholars have developed projects in the recent years to encourage the participation of citizens in the use of public services delivered through IoT in smart cities that have been already implemented in some cities. However, these projects do not involve citizens in the early phases of the design of IoT deployment. A comprehensive sustainable approach including environmental and data security implications of using IoT in smart cities is still missing.

Participatory approaches have been used to engage citizens in the design of smart cities as well as to avoid the potential exclusion or mistrust of technologically focused smart cities projects. Departing from this idea and discussing recent research results about data protection and security as well as about the environmental issues in smart cities, I have explained the development of a participatory approach with a socio-technical processual methodology combining qualitative and quantitative methods of social research as well as visualization and game design.

This framework can be applied in different scenarios of the design of public services using IoT in smart cities as well as in urban setting still attempting to move towards smartification. In contrast to other approaches focusing on technological issues or in citizen engagement with existing innovation, the presented approach departs from a holistic socio-technical perspective including citizens, public

servants and actors involved in the design of IoT and smart cities from the early innovation phases of design. While this approach allows to identify and overcome some risks related to sustainability of the designed smart cities, uncertainties about unexpected uses and security misuse as well as those deriving from the frequently contradictory interconnection between the three sustainability dimensions (social, economic, environmental) (Quack and Ruiz Ben 2004) will remain open. Ongoing revisions of the proposed methods and the design of existing public services delivered through IoT would mitigate this effect (see Table 1) allowing a continuous and inclusive interpretation, evaluation and governance of socio-technical aspects of public service innovations. Another possible risk in the application of this approach is the habituation of repeating the same procedures in public service delivery using IoT ignoring the demands from minority groups. The inclusion of public servants in the cyclic revisions of the design and implementation of public services using IoT is crucial to prevent this risk building a mutual awareness and understanding between the needs of the demand and the delivery actors. All of them are users (Hyysalo and Johnson 2015) of IoT in smart cities even when they use these facilities from different perspectives, motivations, and aims and with different knowledge backgrounds. Moreover, the application of this socio-technical participatory approach would prevent technology-driven enthusiasm and political hyper-activism (Nam and Pardo 2011) and would help to create a community sense of urban places where safety and security can be defined including protecting citizens against feelings of alienation and estrangement.

To conclude, I extract some key recommendations for enriching existing participatory approaches with the proposed framework:

– Include an explorative phase for understanding the particular living logics of the city. Especially in relation to work and transportation, it is crucial to understand how the usage of IoT in public spaces is affecting the change in work habits and mobility. This may vary in different areas of the city and can lead to social segregation. The participatory design of IoT proposed in this chapter raising awareness of the opportunities (and risks) of using these technologies could prevent this effect. This understanding of the living logics of the city goes beyond technology-focused approaches of the design of IoT for public service delivery in smart cities and is also crucial for developing effective governance practices that acknowledge the opportunities and risks of deploying IoT for public service delivery in specific urban settings.
– Include environmental and data security issues. Ahvenniemi et al.'s (2017) have developed a very helpful approach for creating sustainable smart cities. The proposed framework would enrich this approach including data security issues neglected in the design of IoT for public service delivery and in general in smart cities (Kitchin 2016). Many data security risks of IoT for public service delivery in smart cities such as the capture, storage, sharing, and misuse of data produced by these technologies are related to the users' lack of awareness on security. Thus, the inclusion of games in which multiple actors can interact as players and experience as well as discuss digital security aspects of IoT in smart urban contexts would enrich the existing participatory approaches of IoT development and smart cities making.

Possible scenarios for applying the proposed framework are, for example, the design of IoT for public service delivery in small urban settings and suburban spaces. Most of the research of smart cities concentrate on large global cities, neglecting the development of peripheral or distant urban areas. Particularly to prevent social segregation and to ensure that the benefits of using public services through IoT facilities reach every citizen, this approach could be applied in these urban areas. This would also facilitate the establishment of holistic governance approaches for the smartization of public places bringing the citizens to the center of attention. This would mean to go beyond the present focus on global cities and optimistic/opportunistic technology centered "solutions" determined by global technology giants.

References

Ahvenniemi, H., Huovila, A., Pinto-Seppä, I., & Airaksinen, M. (2017). What are the differences between sustainable and smart cities? *Cities, 60*, 234–245. https://doi.org/10.1016/j.cities.2016.09.0090264-2751.

Alford, J., & O'Flynn, J. (2012). *Rethinking public service delivery. Managing with external providers*. London: Palgrave Macmillan.

Avoine, G., et al. (2014). Passengers information in public transport and privacy: Can anonymous tickets prevent tracking? *International Journal of Information Management, 34*(5), 682–688.

Baranauskas, M. C. C. (2014). Social awareness in HCI. *ACM Interactions, 21*(4), 66–69.

Bell, S., Berg, T., & Morse, S. (2016). *Rich pictures: Encouraging resilient communities*. London: Routledge.

Bifulco, F., Tregua, M., Amitrano, C. C., & D'Auria, A. (2016). "ICT and sustainability in smart cities management", *International Journal of Public Sector Management, 29*(2), 132–147.

Bijker, W. E. (1995). *Of bicycles, bakelites and bulbs: Toward a theory of sociotechnical change*. Cambridge, MA: MIT Press.

Bijker, W. E. (2001). Understanding technological culture through a constructivist view of science, technology, and society. In S. H. Cutcliffe & C. Mitcham (Eds.), *Visions of STS: Counterpoints in science, technology, and society studies*. Albany, NY: SUNY Press.

Boring, S., Gehring, S., Wiethoff, A., Blöckner, A. M., Schöning, J., & Butz, A. (2011). Multi-user interaction on media facades through live video on mobile devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM.

Bowker, G., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

Brynskov, M., Carlos Carvajal Bermudez, J., Fernandez, M., Korsgaard, H., Mulder, I., Piskorek, K., et al. (2014). *Urban interaction design: Towards city making*. Amsterdam: Book Sprints.

Buscher, M., Shapiro, D., Hartswood, M., Proctor, R., Slack, R., Voss, A., & Mogensen, P. (2002). Promises, premises and risks: Sharing responsibilities, working up trust and sustaining commitment in participatory design projects. In *Proceedings of the Seventh Biennial Participatory Design Conference* (pp. 183–192).

Caldwell, G. A., & Foth, M. (2017). DIY/DIWO media architecture: The InstaBooth. In A. Wiethoff & H. Hussmann (Eds.), *Using information and media as construction material*. Berlin: DeGruyter.

Chambers, R. (1995). Paradigm shifts and the practice of participatory research and development. In N. Nelson & S. Wright (Eds.), *Power and participatory development*. London: Intermediate Technology Publications.

Cinderby, S. (2010). How to reach the Bhard-to-reach: The development of Participatory Geographic Information Systems (P-GIS) for inclusive urban design in UK cities. *Area, 42*, 239–251.

Cornillie, F., Clarebout, G., & Desmet, P. (2012). The role of feedback in foreign language learning through digital role-playing games. *Procedia - Social and Behavioral Sciences, 34*, 49–53.
Edwards, L. (2016). Privacy, security and data protection in smart cities: A critical EU law perspective. *European Data Protection Law Review, 28*(58).
Firmino, R. J., Kanashiro, M., Bruno, F., Evangelista, R., & da Costa Nascimento, L. (2013). Fear, security, and the spread of CCTV in Brazilian cities: Legislation, debate, and the market. *Journal of Urban Technology, 20*(3), 65–84. https://doi.org/10.1080/10630732.2013.809221.
Fischer, M. (2007). Four genealogies for a recombinant anthropology of science and technology. *Cultural Anthropology, 22*(4), 539–615.
Fischer, P. T., & Hornecker, E. (2012). Urban HCI: Spatial aspects in the design of shared encounters for media facades. In *Proceedings of Human Factors in Computing Systems*. New York: ACM.
Foth, M., Choi, J. H., & Satchell, C. (2011). Urban informatics. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*. New York: ACM.
Foth, M., Brynskov, M., & Ojala, T. (Eds.). (2015). *Citizens right to the digital city: Urban interfaces, activism and placemaking*. London: Springer.
Fredericks, J., Tomitsch, M., Hespanhol, L., & McArthur, I. (2015). Digital pop-up: Investigating bespoke community engagement in public spaces. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*. Melbourne: ACM.
Fredericks, J., Hespanhol, L., & Tomitsch, M. (2016). Not just pretty Lights: Using digital technologies to inform city making. In *Proceedings of the 2016 Media Architecture Biennale*. Sydney: ACM.
Fredericks, J., Hespanhol, L., Parker, C., Zhou, D., & Tomitsch, M. (2017). Blending pop-up urbanism and participatory technologies: Challenges and opportunities for inclusive city making. *City, Culture and Society, 12*, 44–53.
Fraser, E. D. G., Dougill, A., Mabee, W., Reed, M. S., McAlpine, P. (2006). Bottom up and top down: analysis of participatory processes for sustainability indicator identification as a pathway to community empowerment and sustainable environmental management. *Journal of Environmental Management 78*(2), 114–127.
FTTH Council of Europe. (2015). *FTTH smart guide*. Brussels: Council of Europe.
Gabrys, J. (2014). Programming environments: Environmentality and citizen sensing in the smart city. *Environmental Plan and Social Space, 32*(1), 30–48.
Gascó, M. (2016). What makes a city smart? Lessons from Barcelona. In *HICSS '16 Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 2983–2989).
Geser, H. (1990). Organisationen als soziale Akteure. *Zeitschrift für Soziologie, 19*, 401–417.
Greater London Authority. (2016). *The future of smart. Harnessing digital innovation to make London the best city in the world*. London: Greater London Authority.
Hespanhol, L., & Tomitsch, M., (2015). Strategies for Intuitive Interaction in Public Urban Spaces. *Interacting with Computers, 27*(3), 311–326.
Hespanhol, L., Tomitsch, M., McArthur, I., Fredericks, J., Schroeter, R., & Foth, M. (2015). Vote as you go: Blending interfaces for community engagement into the urban space. In *Proceedings of the 7th International Conference on Communities and Technologies*. New York: ACM.
Hoggenmüller, M., & Wiethoff, A. (2014). LightSet: Enabling urban prototyping of interactive media façades. In *Proceedings of 2014 ACM Conference on Designing Interactive Systems*. New York: ACM Press.
Hollands, R. G. (2008). Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City, 12*(3), 303–320.
Hyysalo, S., & Johnson, M. (2015). The user as relational entity. *Information Technology & People, 28*(1), 72–89.
Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management, 29*(4), 258–268.
Janssen, M., Matheus, R., & Zuiderwijk, A. (2015). Big and open linked data (BOLD) to create smart cities and citizens: Insights from smart energy and mobility cases. In *International Conference on Electronic Government* (pp. 79–90). Cham: Springer.

Jing, Q., Vasilakos, V. A., Wan, J., Lu, J., & Qiu, D. (2016). Security of the internet of things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501.

Kitchin, R. (2016). *Getting smarter about smart cities: Improving data privacy and data security*. Dublin, Ireland: Data Protection Unit, Department of the Taoiseach.

Kushner, D. (2013, February). The real story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. *IEEE Spectrum*.

Laamarti, F., Eid, M., & El Saddik, A. (2014). An overview of serious games. *International Journal of Computer Games Technology, 2014*, 358152.

Latour, B. (1999). The trouble with Actor Network Theory. *Soziale Welt, 47*, 369–381.

Lee, J. H., Hancock, M. G., & Hu, M. (2013). Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco. *Technological Forecasting & Social Change, 89*, 80–99.

Löw, M. (2008). The constitution of space: The structuration of spaces through the simultaneity of effect and perception. *European Journal of Social Theory, 11*, 25–49.

Löw, M. (2012). The intrinsic logic of cities: Towards a new theory on urbanism. *Urban Research & Practice, 5*(3), 303–315. https://doi.org/10.1080/17535069.2012.727545.

Madner, V., Mayr, S., Prochazka, K., Hollaus, B., & Hartlieb, J. (2012). Smart cities from a legal and governance perspective. In *Smart city*. Vienna: Schmid Verlag.

Marsal-Llacuna, M. L., & Segal, M. E. (2016). The Intelligenter Method (I) for making "smarter"city projects and plans. Cities, 55, 127–138.

Memarovic, N., Elhart, I., & Langheinrich, M. (2011). FunSquare: First experiences with autopoiesic content. In *Proceedings of the 10th International Conference on Mobile and Ubiquitous Multimedia*. New York: ACM.

Mitchell, V., et al. (2015). Empirical investigation of the impact of using co-design methods when generating proposals for sustainable travel solutions. *CoDesign*. https://doi.org/10.1080/15710882.2015.1091894.

Nam, T., & Pardo, T. A. (2011). Conceptualising smart city with dimensions of technology, people and institutions. In *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times* (pp. 282–291).

Pereira, G. V., Macadar, M. A., Luciano, E. M., & Testa, M. G. (2017). Delivering public value through open government data initiatives in a Smart City context. *Information Systems Frontiers, 19*(2), 213–229.

Popescu, D., & Radu, L. D. (2016). Data security in smart cities: Challenges and solutions. *Informatica Economică, 20*(1), 29–38.

Quack, D., & Ruiz Ben, E. (2004). Sustainable evolution of E-Solutions. Bewertungsmethodik innovativer I&K Konzepte für die sozialökologische Transformation der Informationsgesellschaft. *SEE Report—BMBF-Bundesministerium für Bildung und Forschung*.

Raybourn, E. M. (2014). A new paradigm for serious games: Transmedia learning for more effective training and education. *Journal of Computational Science, 5*(3), 471–481.

Robinson, J., & Cole, R. (2015). Theoretical underpinnings of regenerative sustainability. *Building Research and Information, 43*(2), 133–143. https://doi.org/10.1080/09613218.2014.979082.

Ruiz Ben, E., (2017). *Visualisation methods for the analysis of the digitalisation of work*. Workshop, Open University and University of Oxford, Department of Geography.

Sanders, L., & Stappers, P. J. (2014). From designing to co-designing to collective dreaming: Three slices in time. *Interactions, 21*, 24–33.

Schroeter, R., & Foth, M. (2009). Discussions in space. In *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group*. Melbourne: ACM.

Shin, Y., Shin, D. (2012). "Community informatics and the new urbanism: incorporating information and communication technologies into planning integrated urban communities." *Journal of Urban Technology, 19*(1), 23–42.

Talari, S., Shafie-khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. P. S. (2017). A review of smart cities based on the internet of things concept. *Energies, 10*, 421.

Taylor, N., Marshall, J., Blum-Ross, A., Mills, J., Rogers, J., Egglestone, P., et al. (2012). Viewpoint: Empowering communities with situated voting devices. In *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems*. New York: ACM.

Tomitsch, M., & Haeusler, M. H. (2015). Infostructures: Towards a complementary approach for solving urban challenges through digital technologies. *Journal of Urban Technologies, 22*(3), 37–53.

Turcu, C. (2013). Re-thinking sustainability indicators: Local perspectives of urban sustainability. *Journal of Environmental Planning and Management, 56*(5), 695–719. https://doi.org/10.1080/09640568.2012.698984.

van Waart, P., Mulder, I., & Bont, C. (2016). A participatory approach for envisioning a smart city. *Social Science Computer Review, 34*(6), 708–723.

Vienna City Administration. (2014, July). *Smart City Wien: Framework strategy*. Retrieved March 20, 2018, from https://smartcity.wien.gv.at/site/files/2014/09/SmartCityWien_FrameworkStrategy_english_doublepage.pdf.

Wolff, A., Barker, M., & Petre, M. (2017). Creating a Datascape: A game to support communities in using open data. *8th International Conference on Communities and Technologies*, 26–30 Jun 2017, Troyes, France.

Zambom Santana, E. F., Macedo Bastista, D., Kon, F., & Milojicic, D. S. (2016). SCSimulator: An open source, scalable smart city simulator. *Tools Session of the Brazilian Symposium on Computer Networks*.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.

Zelt, T. (2017). *Smart city, smart strategy. Cities around the world are embracing the digital revolution. But how well are they really doing?* Munich: Roland Berger.

Zyda, M. (2005). From visual simulation to virtual reality to games. *Computer, 38*(9), 25–32.

Esther Ruiz Ben holds the position of private docent at the Institute of Sociology of the Technical University of Berlin, Germany. Her research areas include professionalization and digitalization processes of work in the private and public sector, categorizations of work and social inequalities, innovation and technology, innovation and sustainability as well as the development of research methodologies combining social and computing techniques. Her last book "Internationale Professionalität: Transformation der Arbeit und des Wissens in Transnationalen Arbeitsfeldern" (International Professionalism: Transformation of Work and Knowledge in Transnational Work Fields) has been recently published by Springer.

Identifying Security Challenges in the IoT for the Public Sector: A Systematic Review

Ahmet Guler and Fatih Demir

Abstract This chapter reviews the expanding role of the Internet of Things (IoT) in our lives as well as the security concerns of IoT. While IoT has expanded enormously in recent years both in the private and public sectors where it has enhanced the quality of life, it has also created potential security risks for users in various ways, such as in enabling unauthorized access and misuse of personal information, facilitating attacks on other systems, and creating safety risks. Even though these risks have been already common in cyberspace contexts, the introduction of IoT has increased these risks given its role in expanding the Internet and its connections to every aspect of our daily lives. This chapter will provide a systematic review of the current literature of IoT in order to identify IoT security challenges, and to offer recommendations for responding to these challenges. As a result of our study, we identified pervasiveness, privacy, and vulnerability as main challenges that are discussed in the literature. In this research, we also compiled some recommendations such as encryption, cryptology, authentication, authorization, and advanced security frameworks, schemes, and protocols to respond current security challenges in the IoT. Policy recommendations are also discussed to give ideas to policymakers about IoT security.

Keywords Internet of Things (IoT) · IoT in public sector · Security challenges · Recommendations for IoT security

Abbreviations

AI	Artificial intelligence
AR	Augmented reality

A. Guler (✉)
Pennsylvania State University, University Park, PA, USA
e-mail: aguler@psu.edu

F. Demir
Northern Illinois University, DeKalb, IL, USA
e-mail: fdemir@niu.edu

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_4

DDoS	Distributed denial of service
FTC	Federal Trade Commission
ICT	Information communication technologies
IoT	Internet of Things
IP	Internet protocol
IT	Information technology
MCI	Mass casualty incident
RFID	Radio frequency identification

Introduction

The Internet of Things (IoT) provides many opportunities and new ways of facilitating our lives through smart applications and devices. There has recently been an exponential growth in IoT, which has created huge benefits, not only in our personal lives but also in the realm of public services. While we enjoy having IoT benefits at home such as its ability to help in reducing energy costs, increase home security, and enhance quality of life, IoT also provides benefits in the context of smart city projects, areas of industrial growth and improvement, and environmental protection. However, the use of IoT applications in every aspect of our daily lives has raised security concerns due to their vulnerability to cyberattacks and possible misuse. As of today, it is a fact that a total of three billion people, which represents 40% of the world's population, are connected online. Researchers assume that by the year 2020, at least 40 billion more devices will be connected to each other via the online network. Meantime, IoT is being increasingly recognized by groups in the private sector, as well as by various government agencies to provide better services to people. IoT increases not only the efficiency of equipment but also quality of life, in situations such as healthcare, the monitoring of critical processes, and operations in complex workflows (Demir et al. 2017).

The current increase in the use of sensors to integrate many complex processes has made it easier to manage multiple systems remotely. This has permitted some possible opportunities for better outcomes, including, but not limited to, smart transportation, medical communication devices, smart houses, and smart cities. IoT affords many opportunities to make people's lives easier; therefore, IoT is a very attractive topic for gathering the interests of technology developers, innovative entrepreneurs, and researchers. It is thus inevitable that the impact of IoT will significantly influence the lives of most citizens, while changing the nature of the provision of public services. However, it poses its own security challenges due to the well-known vulnerability of the internet as an insecure device. As well, the complex typology of the IoT network and the interaction between various devices poses additional security threats. The digitally networked world is also open to cyberattacks, and the cost of preventing these attacks is expected to reach about 3 trillion USD by 2020 (Chinn et al. 2014). This chapter provides a systematic literature review of this topic in order to help the reader to better understand the current debates about the security challenges of IoT, and offers recommendations to reduce its security risks.

Background

Contemporary modern life is fostering a high penetration of Information Communication Technologies (ICT) based solutions in order to make people's lives more comfortable and of better quality. The development of ICT and emerging devices has also brought a new term into our lives, namely, the "Internet of Things (aka IoT)." Although there are various definitions used to describe IoT, the term mainly refers to the technological solutions that can be reached with advanced technology, including, but not limited, to RFIDs, sensor networks, machine-to-machine communications (Atzori et al. 2017). Interconnectivity between these devices has hence become a major component of daily life. By increasing its effectiveness, efficiency and expanding opportunities, and by empowering people through technology and Artificial Intelligence (AI) IoT also has the potential to create an effective ecosystem (Berman and Cerf 2017).

The International Telecommunication Union (ITU) has set forth its definition of the Internet of Things as, "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" (Wortmann and Fluchter 2015, p. 221). According to the Radio Frequency Identification (RFID) group, the Internet of Things defined as "the worldwide network of interconnected objects uniquely addressable based on standard communication protocols" (Gubbi et al. 2013, p. 1648). The Cluster of European Research Projects on the Internet of Things defines IoT as "things are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running process that trigger actions and create services with or without direct human intervention" (Sah 2016).

A number of recent developments in ICT technologies have specifically influenced the definition of IoT, such as its referral to connectivity and various kinds of computing devices. On the other hand, many stakeholders define IoT by referring to an internet-oriented or a things-oriented perspective. Besides this, some researchers have defined IoT basically as a formula including Services + Data + Networks + Sensors = IoT (Wainwright 2015). Later, much broader definitions entered the literature, and these referred to ubiquitous computing, internet protocol (IP), machine-to-machine, cutting edge technology and embedded devices, and the Internet of People which encouraged the use of the inclusive term IoT to replace all the previous descriptions (Atzori et al. 2017). IoT technologies incorporate not only hardware but also networking devices and the existing hardware. Smart housing appliances such as smart TVs, thermostats, light fixtures, smart ovens which embrace technologies have considered shifting the term IoT to such devices where every appliance is then networked with a specific IP address (Hahn 2017).

One of the missions of governments is to improve the delivery of effective public services, and to do this efficiently, while meeting the expectations of citizens (Demir 2011). The U.S. Senate Committee on Commerce, Science, and

Transportation has addressed the needs and advances of smart technology and use of IoT in various ways such as the use of IoT automotive technologies in transportation, cell phone, and communication technologies. Thus, the Senate encourages innovation and competition in advancing the emerging technologies to increase the quality and safety of the citizenry (Thune et al. 2008). Survey research results, in the countries of Australia, Finland, France, Germany, Japan, Norway, Singapore, the UK, and the USA, show that emerging technologies are already playing a significant role in helping agencies achieve their mission and demands for future gains are high (Public Accenture 2016).

Recent developments in ICT and the IoT have also strongly influenced the implementation of public administration processes. Thus, local and federal governments have considered adjusting public services accordingly, including, but not limited to, their human activities and services such as transportation, health care, the natural environment, the built infrastructure, education, retail enterprises, industry, and governance (Scholl 2016). For instance, the UK government recently invested $38 million in order to increase the IoT capabilities of the private sector in realm of security and trust, data interoperability, design and development (Harrop 2016). It is true that tomorrow's technology will be fast, and smart and will increase the efficiency of human life. IoT can serve in diverse situations from flood control in Texas, to wildlife protection in Los Angeles (Harbert 2017). In regards to library services, research shows there is ample room for the implementation of IoT in libraries in terms of user engagement, collections and in-service points as well as space usage and users' decision-making processes based on the evidence.

In recent years, ICT has been leveraged in building promising opportunities to develop powerful industrial systems and applications by powering the ubiquity of radio frequency identification (RFID), and mobile, sensor based and wireless devices (Demir 2012). Developments in ICT and IoT have incorporated complex Information Technology (IT) systems equipped with sensing, identification, processing, communication and networking capabilities (Demir 2014). Industry has had a strong interest in deploying such technology to integrate applications such as monitoring, control, data analysis, management, and maintenance. For instance, in Germany, Bosch piloted a real time parking lot management system by using the IoT sensors. The system automatically identifies available spots on the parking lot and posts them on the website with pricing information and thus, makes visible for drivers where they can park and how much they will have to pay (Warburton 2015).

Most governments have initiated the creation of smart cities to promote a large-scale planned urbanization and to support accelerated growth and development by empowering services through advanced technology and quality of services to the citizenry (Gil-Garcia et al. 2015; Suresh and Ramachandran 2016). Van den Bergh and Viaene (2015) examined the implementation of key challenges in smart city initiative in the city of Ghent in Belgium. They proposed the smart city as an ecosystem, in which the local government has to meet the challenge of determining its role in the ecosystem. It was suggested that the local government assign a relatively well-qualified person to an administrative position in order to bridge the system boundaries, as well as considering a stricter form of governance that would allow for

cross- and interdepartmental interactions and initiatives (Van den Bergh and Viaene 2015). It has also been argued that strategies of the governments in building smart cities need to support resilient urban designs, equitable land management, and an integrated infrastructure in the most effective ways (Suresh and Ramachandran 2016).

Government agencies are also implementing projects using the emerging technologies of IoT. During any mass casualty incident (MCI) two-way communication between first medical responders in the field and medical incident commanders at the site are critically important for reducing mortality rates and for coordinating the available resources. All types of detailed information at the time of disasters also need to be effectively and efficiently presented through intelligent user interfaces. Such interfaces need to be "easy-to-use" by Incident Commanders in order to foster critical decisions that can potentially save people's lives. A next-generation multiple casualty management system aka, Panacea's Cloud™ has been iteratively developed and refined based on user experience research driven methodology that employed a mixed methods approach, including the views of clinical experts. Panacea's Cloud™ is an example of a next generation MCI system which has an intelligent dashboard that integrates the IoT technologies such as wearable devices and Augmented Reality technology (AR), virtual beacons and sensor network nodes. It supports coordination between Incident Commanders and paramedics. The research demonstrates how IoT-based web applications, especially AR and the use of smart glasses can be futuristically designed for purposes of smart healthcare applications that have effective and efficient communication capabilities. The development process of the system includes incorporating situational awareness features, a Synchronous Map View system, a Hands-Free Communication service with AR and smart glasses, Digital Notes and resilient Wi-Fi network (Demir et al. 2017).

Providing safety and security is the critical responsibility of governments. Police departments around the world use cutting-edge technologies to fight against crimes and to provide safety for their citizens in an efficient and effective way. For example, smart public safety applications assist police departments to collect and analyze real-time data from streets and other public places in efforts to respond criminal activities and other nuisances and disorders (Kula and Guler 2015). IoT reporting services also increase situational awareness for law enforcement agencies, such as in the reporting of vehicle speeds, engine temperatures, and geolocation information of incident commanders on the field. Such real time information enables law enforcement agency administrators to have a better overview of their jurisdiction, and real time data to minimize operational conflicts between teams working simultaneously to coordinate between other government agencies (Fitzgerald and Kelly 2016). For example, in South Korea, sensor based cameras are used to detect pedestrians' movement and to track suspicious activities in order to prevent crimes and also for scientifically investigating crimes (Jeon and Jeong 2016).

Citizen engagement in the development cycle of IoT projects is crucial for success of the products. Because existing users always provide beneficial feedback based on their previous experience and may offer smart solutions to solve the problems. Engagement of existing users in development and design cycle helps designers to achieve end goals to created better products (Demir 2012). In the state of Washington,

the citizens who use public transportation were invited to co-design public transportation system to identify the current issues, and to develop better ecosystem for all. The research result shows that citizens as co-designers predominantly helped to increase service's behaviors and visualization of the public transportation system (Public Accenture 2016). However, there are some debates over IoT regarding its potential risks in the literature, since it requires a certain understanding of computer use, ability to use and to have access to it. Thus, IoT raises the need for more advanced computer literacy of the entire population so that no one will be left behind because they lack the necessary computer literacy skills (Lindqvist and Neumann 2017).

Research Methodology

This study uses the systematic literature review approach (Cooper 1984) in order to survey the results in the extant literature about IoT security and identify recommendations to ensure security in the IoT. As a research methodology, a systematic literature review can provide invaluable information about what the current knowledge is concerning IoT security and what needs to be done to fill the gaps in the literature. Moreover, a systematic literature review is a highly necessary methodology for assessing the current knowledge and future research areas of emerging topics such as IoT security. To execute our research in a systematic manner, several steps were followed during our research as depicted in Fig. 1.

In the first step of the systematic review, we identified the research questions for the study. The first research question is, "What types of IoT security challenges are raised in the extant literature?" and the second research question is "What types of recommendations are offered for responding to IoT security challenges?" To conduct the search using the current literature, we decided to employ "IoT security" as a search keyword. We used this word both in combination, as well as separately in order to maximize our search results. We conducted our search using three main databases; Science Direct, Google Scholar, and EBSCOhost, in an effort to obtain peer-reviewed journal articles. While doing our search from these databases, we only included articles written in English, published in peer-reviewed journals, and that directly focused on IoT security between 2010 and 2018. While executing a search in each database, we looked for "IoT security," "IoT," and "security" in the title, abstract, and keywords of each research article. After retrieving articles from these databases, we started an initial review to exclude any duplication, conference proceeding, or articles from magazines and other nonacademic outlets. After our initial review, we started to look at each research article carefully to find answers to our defined research questions. During this step, we also classified articles according to research methodology, specific research technique, sector, IoT security concerns and issues, and their recommendations and solutions.

At the end of our systematic review, we crosschecked each other's analysis in order to increase consistency and validity in our research. Table 1 summarizes the systematic review in terms of databases and numbers of articles that are retrieved from the databases and numbers of articles that are included in the study.

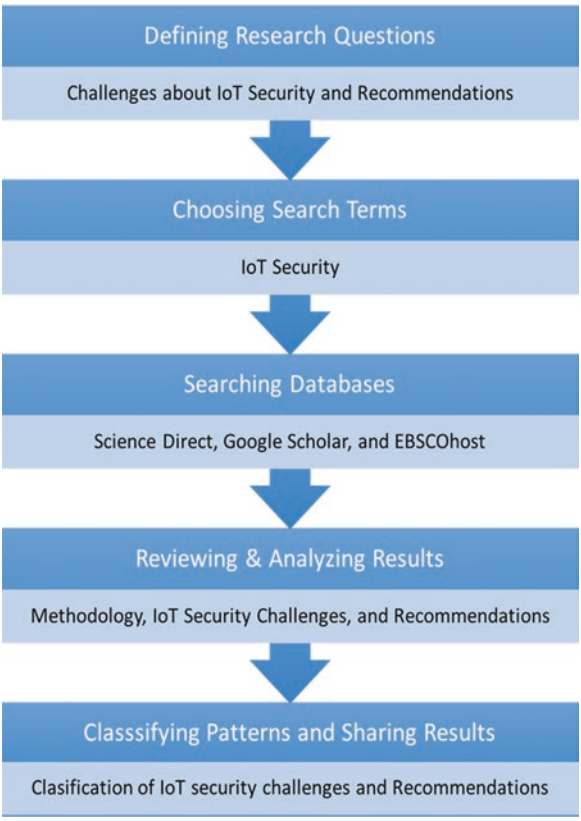


Fig. 1 Systematic literature review steps

Table 1 Databases and retrieved articles

Database	# Retrieved articles	# Included
Science Direct	115	81
Google Scholar	63	44
EBSCOhost	38	32
Total	216	157

Results

In this section, we share the results from our systematic literature review. First, we provide results concerning research methodology, specific research technique, and sector discussed. Then, we discuss findings for our research questions related to IoT security challenges and recommendations to respond these challenges. As discussed in the section below (see section "Security Challenges in IoT"), the results of our systematic literature review indicate that scholars perceive several security challenges related to IoT security such as pervasiveness, privacy, and vulnerability, and also provide critical recommendations to respond these challenges.

According to our classification of current research on IoT security, while the majority of studies (66%, 88 articles) used quantitative research methodology, nearly 34% (69 articles) applied qualitative research methodology. While quantitative studies mainly aimed to develop and test new security schemes, frameworks, models, and policies, qualitative studies surveyed extant literature to understand the current knowledge about IoT security and identify gaps for future research. When we look the topic of each research article to better understand their sector, while nearly 83% of articles did not focus on a specific sector, nearly 6% of articles were written about smart healthcare, 5% of them were about smart home and buildings, 1% were about smart grids and energy, and a further 1% were about smart autos.

After sharing the results from our analysis about the general overview of IoT research, we will now discuss the findings related to our research questions. First, we share the results about our findings related to security challenges in IoT and then we discuss recommendations and solutions offered from our systematic literature review.

Security Challenges in IoT

According to our analysis from our systematic review, we identified several security challenges and recommendations to respond these challenges. As mentioned in the "Research Methodology" section, we looked for answers for "What types of IoT security challenges raised in the extant literature?" and "What types of recommendations are offered to respond to IoT security challenges?" As a result of our review, we identified "pervasiveness, privacy, and vulnerability" as main challenges discussed in the literature. As outlined in the systematic literature review steps of this study above (see Fig. 1), these security challenges have emerged as main issues in the literature when we systematically review and code them according to their approach to IoT security issues and their viable solutions.

Pervasiveness As discussed in the literature, IoT has expanded enormously in the recent years (Ammar et al. 2018). IoT provide many opportunities for to improving services provided by private and public organizations. There are several innovative applications to enhance the quality of life through "smart" applications such as baby monitors, prescription reminders, activity trackers, monitors for an aging family member, sensors and monitors for home utilities, smart city applications, industry development applications, and monitors and sensors for protecting the environment. While IoT provides many opportunities to improve every aspect of our lives, it is also becoming an attractive target for hackers (Hossain et al. 2015). Connecting more devices to the Internet through Wi-Fi networks opens up new possibilities for cybercriminals to attack and steal information from our computers and other digital devices. The vulnerabilities of IoT provide opportunities for hackers to compromise not only the IoT devices but also all connected devices and computer systems through Wi-Fi network connections. According to the Federal Trade Commission

Report (2015), IoT devices have increased the potential risks in the cyberspace for consumers in different ways such as enabling unauthorized access and misuse of personal information, facilitating attacks on other systems, and creating safety risks (FTC 2015, p. 10) Even though these security issues were prevalent in traditional computer systems and in the Internet, the IoT has heightened these risks due to its extension of the Internet to not only traditional systems, mobile networks, and sensor networks but also every "thing" through the Internet connection and communication with each other (Suo et al. 2012). As discussed as a security challenge (Mahmoud et al. 2015), IoT has a heterogeneity feature which connects device to device, human to device, and human to human. However, this feature brings the issues of ensuring security for different devices, different situations, and different functions to our attention.

As a recommendation for responding to challenges related to the pervasiveness and heterogeneity of the data, some scholars offer encryption (Bokefode et al. 2016), cryptology (Bhabad and Bagade 2015; Mai and Khalil 2017; Marin et al. 2015; Mathur et al. 2016; Sanchez-Arias et al. 2017; Schurgot et al. 2015; Zhang et al. 2014), and peer-to-peer networking (Want et al. 2015) to ensure data security and privacy in IoT devices. Several researchers especially argue to use blockchain approaches in IoT (Banerjee et al. 2017; Khan and Salah 2018; Kshetri 2017). While blockchain procedures ensure security in cryptocurrencies, it can provide a more secure communication between IoT devices.

Privacy As a privacy issue of IoT, unauthorized access and misuse of personal information, can occur when hackers utilize weak or absent security measures to reach and collect personal information from IoT and its connected devices (FTC 2015). Hackers try to access computers and its networks, and new smart gadgets such as smartphones, smart TVs, and smart home security. Provide new venues and opportunities for hackers due to their connection to Wi-Fi or cable Internet. Hackers can easily exploit vulnerabilities in these devices to steal sensitive personal information to commit cybercrimes such as identity theft and fraud. Clearly, the increasing demand to make our homes and offices smarter through IoT devices can be expected to lead to more security issues related to unauthorized access and misuse of personal information. For example, a team of hackers were able to steal Gmail account credentials from a smart refrigerator which is synchronized by the user with Gmail Calendar at the Def Con Security Conference in an IoT hacking challenge (Neagle 2015). In order to prevent security breaches and reduce the risks of personal information theft, both public and private organizations need to ensure security and privacy requirements for IoT devices such as resilience to attacks, data authentication, access control, and client privacy (Weber 2010).

In order to protect user privacy in IoT, scholars offer better encryption (Belguith et al. 2018; Yang et al. 2017), more secure frameworks and schemes (Han et al. 2018; Hernandez-Ramos et al. 2015; Sicari et al. 2016; Wang 2018), and enhancement for current security systems (Abomhara and Køien 2014; Jayaraman et al. 2017; Yang et al. 2018). Specifically, some researchers see cloud computing as a solution for "big data" (Bokefode et al. 2016; Jiang et al. 2014). As IoT devices collect tons of

information about our habits, activities, preferences, and daily routines, protecting this sensitive information could be performed through cloud computing services which provide secure databases and storages.

Vulnerability IoT devices may create security vulnerabilities through facilitating attacks on other systems connected to the same platform. In cyberspace, hackers use several malwares to initiate attacks on other computers by recruiting other computers as "zombie computers" (Holt et al. 2015). Similarly, IoT devices open new opportunities and possibilities for hackers to exploit these devices to initiate attack on other connected devices (Sha et al. 2018). For example, hackers recently initiated a series of Distributed Denial of Service (DDoS) attacks against the Domain Name System in order to disrupt internet activities in the U.S. on October 21, 2016. These attacks were made possible by the large number of unsecured IoT devices, and these devices were easily compromised by hackers and infected with a malware to form a botnet. This attack caused a massive disruption of online activities for several hours and generated unnecessary online traffic to make targeted servers busy (Cobb 2016).

Moreover, IoT devices might be compromised by hackers by exploiting security vulnerabilities in order to physical harm the intended users (FTC 2015). For example, there are some white hat hackers try to identify the vulnerabilities of car companies and they successfully accessed the Jeep's computer system to manage its driving functions such as steering, brakes, transmission, and engine with a remote access through a laptop computer (Greenberg 2015). Even though car manufacturers are quick to respond to these zero day exploits, there are still security issues for drivers (Riel et al. 2017). Especially, companies in the automotive industry and IT are in a race to invent a driverless car which depends on sensors, computers, and automation nowadays. However, according to experts, this may also create vulnerabilities to be exploited by hackers (Greenberg 2017). Similarly, proliferation and expansion of smart home devices also creates safety risks for people (Jacobsson et al. 2016; Riahi et al. 2013). Even though we enjoy having IoT devices at home such as thermostats, refrigerators, washing machines, dishwashers, or even toasters, these devices may be exploited by cybercriminals to harm people living at home (Hernandez-Ramos et al. 2015; Tao et al. 2018). For example, according to the result of a security analysis of 50 smart home devices (Marcena and Wueest 2015), there are several weaknesses in IoT devices such as using weak passwords, not using mutual authentication, or protected accounts against brute-force attacks.

The IoT devices have expanding rapidly and they have still more potential to grow in different aspects of our daily life. However, there should be adequate security and privacy mechanisms built into the design of these devices in order not to see similar issues we face with the Internet today (Mayer 2009). Even though the exponential expansion of the Internet in our everyday lives has created lots of benefits for us, some individuals have subverted its original design to commit crimes and misuse its applications (Holt et al. 2015). We may face similar security issues with IoT if we do not think about security issues at the start of applying these technologies (Wurm et al. 2016). Moreover, there are even more potential risks of IoT devices compared to computers. Even though computers have security risks when connected to the Internet, there are several IT companies and experts to provide security

for computers against any misuse or hacking. However, similar companies are still their infancy in the IoT sector and they do not have enough experience to deal with security issues related to IoT devices. Moreover, some IoT devices are manufactured to function for simple tasks in specific machines or have built-in technologies which do not allow updates of their operating systems. Thus, this may create vulnerabilities for consumers who are not aware of their risks or do not have ability to update security patches on their devices (FTC 2015).

However, there are still chances to provide secure IoT if public and private sectors are willing to ensure necessary actions while designing and initiating IoT. In fact, it is much easier and more efficient to be proactive rather than reactive in efforts to respond to security incidents (Allen 2016). To reduce vulnerability and minimize attacks against IoT devices, scholars urge better security systems which can ensure access control (Bokefode et al. 2016; Gusmeroli et al. 2013; Li et al. 2018, 2016; Hossain et al. 2015), certification (Kang and Kim 2017), authentication (Caron et al. 2016; Dhillon and Kalra 2017; Feng et al. 2018; Kalra and Sood 2015; Kim et al. 2017; Lavanya and Natarajan 2017; Li et al. 2018; Peris-Lopez et al. 2018; Tai et al. 2017; Wang et al. 2017; Wu et al. 2018), and proper authorization (Mineraud et al. 2016; Sanchez et al. 2013; Zhang et al. 2014) for IoT devices.

Conclusion

In this study, we conducted a systematic literature review to better understand current security challenges in IoT and advance recommendations to respond to these challenges. According to our analysis, we identified pervasiveness, privacy, and vulnerability as main challenges that are discussed in the literature. We also compiled some recommendations from the literature review such as encryption, cryptology, authentication, authorization, and advanced security frameworks, schemes, and protocols. As discussed above, security challenges in IoT and recommendations for solving these problems warrant further research to test and examine the feasibility of these recommendations for IoT security.

From a policy perspective, governments should foster a productive collaboration among different stakeholders of IoT such as researchers, academicians, IT practitioners, and other key players in order to ensure innovation while addressing security challenges discussed above. As a policymaker, government entities should function as facilitators among different key players in the ICT sector to realize coordination and standardization in IoT security to ensure security and reduce the risks. Rather than creating rigid regulations and policies, it is better to create policies that are flexible and adaptable to emerging threats and security challenges in the IoT sector (U.S. Department of Commerce 2017).

To sum up, IoT has quickly expanded in every aspect of life and has already created important benefits for our lives. Both public and private organizations use IoT in order to provide better services with reduced costs. It is obvious that we will see more IoT devices in our lives in the near future. However, security risks posed by IoT are much higher than before due to its invasive roles in almost every part of our lives.

Therefore, there should be proper security measures to prevent cyberattacks in order to avoid catastrophic scenarios facilitated via IoT connected networks. As succinctly worded, an ounce of prevention is worth a pound of cure.

References

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. In *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)* (pp. 1–8).

Allen, N. (2016). Cybersecurity weaknesses threaten to make smart cities more costly and dangerous than their analog predecessors. *USApp–American Politics and Policy Blog*.

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications, 38*, 8–27.

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks, 56*, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004.

Banerjee, M., Lee, J., & Choo, K.-K. R. (2017). A blockchain future to Internet of Things security: A position paper. *Digital Communications and Networks, 4*(3), 149–160.

Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., & Attia, R. (2018). PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT. *Computer Networks, 133*, 141–156.

Berman, F., & Cerf, V. G. (2017). Social and ethical behavior in the Internet of Things. *Communications of the ACM, 60*(2), 6–7. https://doi.org/10.1145/3036698.

Bhabad, M. A., & Bagade, S. T. (2015). Internet of Things: Architecture, security issues and countermeasures. *International Journal of Computer Applications, 125*(14), 1–4.

Bokefode, J. D., Bhise, A. S., Satarkar, P. A., & Modani, D. G. (2016). Developing a secure cloud storage system for storing IoT data by applying role based encryption. *Procedia Computer Science, 89*, 43–50.

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review, 32*(1), 4–15.

Chinn, D., Kaplan, J., & Weinberg, A. (2014). *Risk and responsibility in a hyperconnected world: Implications for enterprises*. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises.

Cobb, S. (2016). *10 things to know about the October 21 IoT DDoS attacks*. Retrieved from https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/.

Cooper, H. M. (1984). *The integrative research review: A systematic approach*. Beverly Hills, CA: Sage Publications.

Demir, F. (2011). *Technology use in community policing: Usability evaluation by Eye tracking method*. Germany: Lambert Academic Publishing.

Demir, F. (2012). Designing intranet communication portals for government agencies: Turkish National Police Case. *Police Science Journal*. Retrieved from http://www.arastirmax.com/bilimsel-yayin/polis-bilimleri-dergisi/14/2/75-94-kamu-kurumlari-ic-ag-iletisim-portali-tasarimi-turk-polis-teskilati-ornegi.

Demir, F. (2014). Communication ethics. In *Ethics in professional*. Ankara: Adalet Publishing House.

Demir, F., Ahmad, S., Jiang, D., Huang, R., Jahnke, I., & Calyam, P. (2017). A next-generation augmented reality platform for mass casualty incidents. *Journal of Usability Studies, 12*(4), 193–214.

Dhillon, P. K., & Kalra, S. (2017). A lightweight biometrics based remote user authentication scheme for IoT services. *Journal of Information Security and Applications, 34*, 255–270.

Federal Trade Commission. (2015). *Internet of Things*. FTC Staff Report. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Feng, W., Qin, Y., Zhao, S., & Feng, D. (2018). AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS. *Computer Networks, 134*, 167–182.

Fitzgerald, P., & Kelly, D. (2016). The Internet of Things: What sheriffs need to know. *Sheriff & Deputy, 68*(4), 48–51.

Gil-Garcia, J. R., Pardo, T. A., & Nam, T. (Eds.). (2015). *Smarter as the new urban agenda: A comprehensive view of the 21st century city* (Vol. 11). Cham: Springer.

Greenberg, A. (2015). *Hackers remotely kill a jeep on the highway—With me in it*. Retrieved July 19, 2017, from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Greenberg, A. (2017). *Securing driverless cars from hackers is hard. Ask the ex-Uber guy who protects them*. Retrieved July 19, 2017, from https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling, 58*(5), 1189–1205.

Hahn, J. (2017). The Internet of Things: Mobile technology and location services in libraries. *Library Technology Reports, 53*(1), 5–28.

Han, Q., Zhang, Y., & Li, H. (2018). Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. *Future Generation Computer Systems, 83*, 269–277.

Harbert, T. (2017). Making connections. *Government Technology, 30*(1), 16–20.

Harrop, P. (2016). Benchmarking clarifies the future of Internet of Things. *Database & Network Journal, 46*(6). Retrieved from https://www.mendeley.com/research-papers/benchmarking-clarifies-future-internet-things.

Hernandez-Ramos, J. L., Moreno, M. V., Bernabe, J. B., Carrillo, D. G., & Skarmeta, A. F. (2015). SAFIR: Secure access framework for IoT-enabled services on smart buildings. *Journal of Computer and System Sciences, 81*(8), 1452–1463.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. New York: Routledge.

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the Internet of Things. In *Services, 2015 IEEE World Congress* (pp. 21–28). New York: IEEE.

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems, 56*, 719–733.

Jayaraman, P. P., Yang, X., Yavari, A., Georgakopoulos, D., & Yi, X. (2017). Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Generation Computer Systems, 76*, 540–549.

Jeon, J., & Jeong, S.-R. (2016). Designing a crime-prevention system by converging big data and IoT. *Journal of Internet Computing and Services, 17*(3), 115–128. https://doi.org/10.7472/jksii.2016.17.3.115.

Jiang, L., Xu, L. D., Cai, H., Jiang, Z., Bu, F., & Xu, B. (2014). An IoT-oriented data storage framework in cloud computing platform. *IEEE Transactions on Industrial Informatics, 10*(2), 1443–1451.

Kalra, S., & Sood, S. K. (2015). Secure authentication scheme for IoT and cloud servers. *Pervasive and Mobile Computing, 24*, 210–223.

Kang, S., & Kim, S. (2017). How to obtain common criteria certification of smart TV for home IoT security and reliability. *Symmetry, 9*(10), 233.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.

Kim, K.-W., Han, Y.-H., & Min, S.-G. (2017). An authentication and key management mechanism for resource constrained devices in IEEE 802.11-based IoT access networks. *Sensors (Basel, Switzerland), 17*(10).

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027–1038.

Kula, S., & Guler, A. (2015). Smart public safety: Application of mobile electronic system integration (MOBESE) in Istanbul. In *Smarter as the new urban agenda* (pp. 243–258). Cham: Springer International Publishing.

Lavanya, M., & Natarajan, V. (2017). Lightweight key agreement protocol for IoT based on IKEv2. *Computers & Electrical Engineering, 64*, 580–594.

Li, F., Han, Y., & Jin, C. (2016). Practical access control for sensor networks in the context of the Internet of Things. *Computer Communications, 89–90*, 154–164.

Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K.-K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments. *Journal of Network and Computer Applications, 103*, 194–204.

Lindqvist, U., & Neumann, P. G. (2017). The future of the Internet of Things. *Communications of the ACM, 60*(2), 26–30.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges and prospective measures. In *10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336–341).

Mai, V., & Khalil, I. (2017). Design and implementation of a secure cloud-based billing model for smart meters as an Internet of Things using homomorphic cryptography. *Future Generation Computer Systems, 72*, 327–338.

Marcena, M. B., & Wueest, C. (2015). Insecurity in the Internet of Things. *Security Response, Symantec.*

Marin, L., Pawlowski, M. P., & Jara, A. (2015). Optimized ECC implementation for secure communication between heterogeneous IoT devices. *Sensors (14248220), 15*(9), 21478–21499.

Mathur, A., Newe, T., & Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. *Sensors (14248220), 16*(1), 1–25.

Mayer, C. P. (2009). Security and privacy challenges in the internet of things. *Electronic Communications of the EASST, 17*. https://doi.org/10.14279/tuj.eceasst.17.208.

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. *Computer Communications, 89–90*, 5–16.

Neagle, C. (2015, August 26). *Smart refrigerator hack exposes Gmail account credentials*. Retrieved July 19, 2017, from http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

Peris-Lopez, P., González-Manzano, L., Camara, C., & de Fuentes, J. M. (2018). Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things. *Future Generation Computer Systems, 81*, 67–77.

Public Accenture. (2016). *Smart move: Emerging technologies make their mark on public service among the foremost missions of government is to improve the delivery of public service and meet the rising expectations of citizens*. Retrieved from https://www.mendeley.com/research-papers/smart-move-emerging-technologies-make-mark-public-service-among-foremost-missions-government-improve.

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013). A systemic approach for IoT security. In Distributed Computing in Sensor Systems (DCOSS). In *2013 IEEE International Conference* (pp. 351–355). New York: IEEE.

Riel, A., Kreiner, C., Macher, G., & Messnarz, R. (2017). Integrated design for tackling safety and security challenges of smart products and digital manufacturing. *CIRP Annals, 66*(1), 177–180.

Sah, P. (2016). Saving environment using Internet of Things: Challenges and the possibilities. *Advances in Internet of Things, 6*, 55–64.

Sanchez-Arias, G., González García, C., & Pelayo G-Bustelo, B. C. (2017). Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things. *Future Generation Computer Systems, 74*, 444–466.

Sanchez, P., Lopez, R., & Skarmeta, A. (2013). Panatiki: A network access control implementation based on pana for IoT devices. *Sensors, 13*(11), 14888–14917.

Scholl, H. J. (2016). Special issue on "Smartness in governance, government, urban environments, and the Internet of Things": An editorial introduction. *Information Polity, 21*(1), 1–3. https://doi.org/10.3233/IP-150377.

Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015). *Experiments with security and privacy in IoT networks* (pp. 1–6). New York: IEEE.

Sha, K., Wei, W., Andrew Yang, T., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems, 83*, 326–337.

Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., & Coen-Porisini, A. (2016). A secure and quality-aware prototypical architecture for the Internet of Things. *Information Systems, 58*, 43–55.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A review. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 3, pp. 648–651). https://doi.org/10.1109/ICCSEE.2012.373.

Suresh, P., & Ramachandran, S. (2016). Development of smart cities in India—Dream to reality. *Scholedge International Journal of Business Policy & Governance, 3*(6), 73–81. https://doi.org/10.19085/journal.sijbpg030601.

Tai, W. L., Chang, Y. F., & Li, W. H. (2017). An IoT notion-based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks. *Journal of Information Security and Applications, 34*, 133–141.

Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems, 78*, 1040–1051.

The U.S. Department of Commerce. (2017). *Fostering the advancement of the Internet of Things*. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

Thune, J., Dakota, S., Roger Wicker, C. F., Roy Blunt, M., Marco Rubio, M., Kelly Ayotte, F., Hampshire J., & Moran, N. (2008). *Senate Committee on Commerce, Science, and Transportation One Hundred Fourteenth Congress Second Session Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety and Security*. Retrieved from https://www.mendeley.com/research-papers/senate-committee-commerce-science-transportation-one-hundred-fourteenth-congress-second-session-subc.

Van den Bergh, J., & Viaene, S. (2015). Key challenges for the smart city: Turning ambition into reality. In *2015 48th Hawaii International Conference on System Sciences* (pp. 2385–2394). IEEE.

Wainwright, N. (2015). *Innovate 11 Presentation*. USA: Internet of Things Panel. Retrieved from https://www.postscapes.com/videos/viewvideo/180/innovate-11-internet-of-things-panel/Page-1.

Wang, Z. (2018). A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity. *Future Generation Computer Systems, 82*, 342–348.

Wang, K.-H., Chen, C.-M., Fang, W., & Wu, T.-Y. (2017). A secure authentication scheme for Internet of Things. *Pervasive and Mobile Computing, 42*, 15–26.

Want, R., Schilit, B. N., & Jenson, S. (2015). Enabling the Internet of Things. *Computer, 48*(1), 28–35.

Warburton, S. (2015). Bosch pilots active parking management system. *Aroq—Just-Auto. Com (Global News)*. Retrieved from https://www.mendeley.com/research-papers/bosch-pilots-active-parking-management-system.

Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008.

Wortmann, F., & Fluchter, K. (2015). Internet of Things. *Business & Information Systems Engineering, 57*(3), 221–224.

Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., & Shen, J. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Generation Computer Systems, 82*, 727–737.

Wurm, J., Arias, O., Hoang, K., Sadeght, A., & Jin, Y. (2016). Security analysis on consumer and industrial IOT devices. *21st Asia and South Pacific Design Automation Conference (ASP-DAC)*.

Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health Internet of Things. *Journal of Network and Computer Applications, 89*, 26–37.

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2018). Privacy-preserving fusion of IoT and big data for e-health. *Future Generation Computer Systems, 86*, 1437.

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT Security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications* (pp. 230–234).

Ahmet Guler is assistant teaching professor in the Department of Sociology and Criminology at the Pennsylvania State University and the Director of Graduate Studies in Criminal Justice Policy and Administration. His research focuses on criminal justice policy, policing, terrorism, criminal justice reform, information technology in criminal justice, and transnational crime.

Fatih Demir graduated from the University of Baltimore, earning the degree of Doctor of Communications Design (DCD) in 2009. In August 2015, he served at the School of Information Science and Learning Technologies at the University of Missouri as a postdoctoral fellow for 2 years and then joined the Educational Technology, Research, and Assessment Department at the Northern Illinois University (NIU) as an assistant professor by August 2017.

Dr. Demir has spent years teaching and researching human-computer interaction (HCI), usability, interaction design, social media analysis, and e-government design. He conducted research by deploying remote and mobile eye-tracking systems as well as brain wave monitoring EEG systems at the University of Baltimore, University of Missouri, and Northern Illinois University. As a multidisciplinary researcher, he worked with faculty, staff, and graduate assistants on various projects in the realm of journalism, education, medicine, and computer science.

He is currently teaching User Experience Research and User Experience Design courses at the NIU.

Using Blockchain Technology to Manage IoT Data for Smart City Initiatives: A Conceptual Framework and Initial Experiments Based on Smart Contracts

Lingjun Fan, Felippe Cronemberger, and J. Ramon Gil-Garcia

Abstract Blockchain technology is attracting the interest of professionals and academics across a variety of disciplines, including the interdisciplinary field of digital government. Such technology has the potential to transform the public sector by providing innovative ways to secure data and detect tampering. However, few studies have theorized the experimental applications of such technology and how it could be applied to data management practices in data-rich environments, such as the Internet of Things (IoT) applications in smart cities. This chapter proposes a workflow diagram for technical experiments that explore how blockchain technology can protect the integrity of data from sensors in a context where IoT functions as the underpinning infrastructure. This endeavor helps to contextualize this emerging technology and sheds light on opportunities, risks, and challenges of using blockchain technology in environments where intensive data collection is the norm. Contributions include a framework on data management for IoT that can be of special value to local governments that are considering blockchain as instrumental in engaging in or enhancing data-driven operations.

Keywords Blockchain technology · Internet of Things · Smart contracts · IoT data management

L. Fan (✉)
Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China
e-mail: fanlingjun@ict.ac.cn

F. Cronemberger
University at Albany, State University of New York, Albany, NY, USA
e-mail: fcronemberger@alumni.albany.edu

J. R. Gil-Garcia
University at Albany, State University of New York, Albany, NY, USA

Universidad de las Americas Puebla, San Andrés Cholula, Puebla, Mexico
e-mail: jgil-garcia@ctg.albany.edu

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_5

Abbreviations

ABIs	Application binary interfaces
DAMA	Data Management Association
DDoS	Distributed denial of service
ETH	Ether
EVM	Ethereum Virtual Machine
ID	Identity
IDC	International Data Corporation
IoT	Internet of Things
IP	Internet protocol
IPFS	Interplanetary file system
RPi	Raspberry Pi

Introduction

In this new century, smart city initiatives are being studied as local government's best approach to promoting sustainable industrialization, *informatization*, and urbanization. By envisioning the integration of advanced information and communication technologies such as big data analytics, cloud computing, the Internet of Things (IoT), mobile computing, and artificial intelligence, smart cities represent a vision of local governments that are better equipped to address a number of urban issues, including traffic congestion, pollution, resource shortages, and large population growth. The logic behind a smart city is daring, but simple: solutions can be achieved if the city becomes more connected, more digitalized, and, as the terminology implies, more intelligent (Koh et al. 2015; Meijer et al. 2016).

Smart cities are often portrayed as potentially thriving precisely because of the possibilities that emerge from the integrated use of emerging technologies (Gil-Garcia et al. 2014). For example, while the Internet, IoT, and mobile devices are responsible for collecting data and information, cloud computing may be used to store and process the data. Big data could then be seen as a metaphor for the "brain of a city," a neurological system where data can be transformed into information, information to knowledge, and, finally, knowledge is transformed to intelligence and actions that improve quality of life.

IoT is one of the basic technologies for building a smart city's infrastructure (Zanella et al. 2014). IoT data are essential to understanding how people in cities move, how energy is used, and how various infrastructure components interact. IoT data offer the potential for cities to obtain valuable insights from a large amount of data collected through various IoT devices (Bonomi et al. 2014). By installing more and more IoT devices such as sensors and cameras, as well as distributing wearable

devices in a city, more and more data can be captured and potentially used. The success of smart cities is thereby strongly connected to the effective use of IoT data. The creation of a sensory system for a city is not only about creating Wi-Fi hotspots or implementing data collection devices but also about utilizing IoT to create a networked city that facilitates the free flow of information and data utilization (Rathore et al. 2016).

However, many of the devices used for IoT applications have several limitations regarding performance, storage, and security capabilities. First, it must be observed that more and more devices are connected to the cloud center, causing data transmission and heavy network bandwidth pressure. Further, the existence of a single point of failure may expose the entire system to the risk of failure. In the same context, the fact that data is centralized or controlled by third parties also may lead to issues with data security and privacy leaks. What is more, some real-time applications that need timely feedback may suffer from under-performance due to data delays. Finally, having more connected devices does not ensure trust, making it difficult to implement automated interaction between devices. For instance, the secured transmission of data from IoT devices to a central system for analysis could become challenging and does not have a ready-to-use solution.

This chapter proposes a workflow diagram for an experiment to understand how blockchain technology could enhance the management of data generated by devices connected through an IoT network infrastructure. This new knowledge will help cities to better assess the potential of blockchain technology to secure and manage data produced by sensors, cameras, and other devices.

IoT is one of the basic technologies for building smart cities. Current cloud-based centralized IoT data management has many drawbacks such as that data is totally controlled by a third party or is easily attacked. The emergence of blockchain technology has the potential to provide a distributed form of IoT data management. This chapter investigates the benefits and challenges associated with this endeavor, and it is organized into six sections, including this introduction. Section "Characterizing the Internet of Things and Blockchain" gives an overview of blockchain technology and its potential benefits and challenges for IoT applications. The problems of IoT data governance in its currently popular centralized form are also depicted. In section "Using Blockchain Technology to Enhance IoT Data Management", we talk about prior research related to using blockchain to enhance IoT data management. We propose a case study of IoT data governance based on blockchain technology and describe the design and implementation of the experiments in section "Proposing a Case Study and a Conceptual Experiment". We discuss issues with the experiments in section "Discussion and Implications" and, finally, we present our conclusions and suggest future areas for research on this topic in section "Conclusion".

Characterizing the Internet of Things and Blockchain

This section describes the characteristics of blockchain technology and analyzes the risks and challenges that IoT data management currently faces, including privacy issues and data security problems. The section also provides some ideas about how blockchain technology can contribute to the solution of these problems, including not only its potential benefits but also the main challenges to its implementation that would need to be addressed.

As the interest in the Internet of Things grows and spans a variety of domains, the vision of a world managed and governed by data has finally gone mainstream. From executives to politicians, the realization that the world could be irreversibly seen as "datafiable" opens clear opportunities for progress in challenges like security and urban development. IoT is perceived to have set a new infrastructure paradigm, one that has implications from data scalability and integration (Dalčeković et al. 2017) to the way legacy systems are governed (Rosas et al. 2017).

One of the most daunting challenges involving value extraction from data through IoT involves ensuring security and privacy in data management (Ban et al. 2016; Sicari et al. 2015). The potential risks are many, but two deserve immediate attention. First, data collected through IoT devices are stored in a centralized cloud center. From a risk assurance standpoint, that already exposes a single point of failure (Ranjithprabhu and Sasirega 2014), wherein the entire system may be compromised if one failure occurs because data collection practices are part of a unified system. That could not only be dangerous but also create performance bottlenecks. Second, centralization also involves ownership by a third party, a condition that raises privacy concerns for users and, as the model scales up to larger enterprises like smart cities, to the public at large. To successfully implement IoT, cities should make privacy and security a top priority. It is becoming increasingly clear, therefore, that IoT data management needs a more efficient way of moving smart city agendas forward without compromising the safety and security of the citizens and the infrastructure.

As research on security tries to catch up with fast-paced advancements in ubiquitous computing, one technology in particular has risen to prominence: blockchain. Like many prior experiences with technological innovations, blockchain also seems to be portrayed as "the silver bullet" to many security challenges. Heavily popularized by Bitcoin, blockchain is touted as the next big evolution of the Internet (Marsal-Llacuna and Oliver-Riera 2017), with the ability to disrupt industries (Sikorski et al. 2017; Underwood 2016) and redesign the way data management is done (Anh et al. 2018; Azaria et al. 2016). From finance (Adams et al. 2017) to healthcare (Kuo et al. 2017), to sustainable urban policy design and service delivery (Nguyen 2016; Potts et al. 2017), to engineering (Porru et al. 2017) and military operations (Alcazar 2017), the benefits associated with blockchain include, among others, lower transaction costs (Cocco et al. 2017) and seemingly unprecedented capability to secure data (Park and Park 2017).

As a disruptive technology, blockchain's practical and theorized advantages should not be taken for granted. If it evolves like many other technologies, blockchain should not be seen as a deterministic solution but as an intervention whose success and failure are contingent on the context in which it is implemented (DeSanctis and Poole 1994; Orlikowski 2000). In the light of the risks and opportunities that the adoption of blockchain technology may pose to IoT practices in smart cities initiatives, this chapter addresses the importance of connecting theoretical examinations of blockchain technology (Li et al. 2018; Ouaddah et al. 2016) with the growing need for empirical research (Risius and Spohrer 2017). We therefore propose an experiment that, by simulating how blockchain may be enacted for IoT data management, delivers insights on the opportunities and limits of the technology that are worthy of exploration. In the following sections, we present a framework to test blockchain-mediated IoT for data management. This theoretical approach includes the methods for the current experiment and concludes with a path for future experiments in different contexts.

Blockchain Definitions and Rationale

Discussions about blockchain technology have become very common. Although still an emergent technology, its importance seems to go beyond immediate applications across a multitude of domains and industries. It could also promote a cultural shift in the way humans interact with computation in a digital society (Eldred 2016; Swan 2015), problematize the notion of well-established concepts such as monetary currency (Bjerg 2016), and revolutionize the way transactional processes are designed and conducted (Rahim et al. 2018).

While blockchain has been described in many ways and from different perspectives, all definitions seem to converge on the same idea. For example, Risius and Spohrer (2017) claim that blockchain is a "fully distributed system for cryptographically capturing and storing a consistent, immutable, linear event log of transactions between networked actors." Similarly, Li et al. (2018) suggest that blockchain technology enables "historical fabric underneath recording everything that happens exactly as it occurs". Blockchain has also been referred as a technology that aims at creating a network of data (Tapscott and Tapscott 2017) that, by operating in a decentralized fashion and being monitored by multiple parties, publicly and consistently keeps track of transactions and contracts being made. Finally, blockchain could be considered a technology that provides a smart way of making contracts or a "smart contract" technology (Buterin 2014; Glaser 2017).

Conceptually, blockchain technologies are a continuously growing list of blocks and each block contains a set of transactions and a hash of the previous block to link the history of transactions and create an immutable set of records. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way (Di Pierro 2017; Olnes et al. 2017). The block's goal is to record some or all recent transactions. Each time a block is verified and

completed, a new block is generated and added to the blockchain as a permanent database. The blocks are added through cryptography (Ibba et al. 2017; Olnes et al. 2017). There are a countless number of such blocks in the blockchain, and every block contains a hash of the previous block. The blockchain has complete information about different user addresses and their balances right from the genesis block to the most recently completed block. A *genesis* block is the first block of a blockchain, and it does not reference a prior block.

Essentially, a blockchain consists of two functional elements: transactions and interactions (O'Leary 2017; Olnes et al. 2017). Transactions are the actions created by the participants in the system. Blocks register these transactions and make sure they are in the correct sequence and have not been tampered with. Blocks also record a *timestamp* when the transactions were added. All the participants in the network have to reach a consensus to accept transactions (Kraft 2016), allowing all participants to keep track of the transactions without a dominant recordkeeping system. Each node—a computer connected to the network—gets a copy of the data and, by storing data across its network, blockchain sets out to eliminate the risks that come with data being held centrally.

Potential Benefits of Blockchain

Research has been prolific at pinpointing blockchain technology benefits. For example, blockchain has been described as a "universal trustless database" (Huckle et al. 2016), "considered by many impossible to corrupt" (Carlozo 2017), a "driver of social change" (Giungato et al. 2017), and a technology with "an unprecedented degree of surveillance and control" (Smolenski 2018a). Blockchain is also known to bring forth "publicly auditable content" (Huckle and White 2017), and is resilient against threats to data, such as theft (Alcazar 2017; Biswas and Muthukkumarasamy 2016). Finally, blockchain may promote an institutional revolution in participation and decision-making (Aste et al. 2017; Swan 2015) and may improve governance systems through overcoming the centralization of IoT solutions (Marsal-Llacuna 2018).

References to the advantages of using such technology are considered interdisciplinary. According to Kshetri (2017b), its possible advantages include the ability to detect fraud by accurately indicating "the party at fault" and may even "stimulate access to financial services for disadvantaged groups". It has also been suggested that blockchain may improve supply chain performance in a globally competitive environment (Debabrata and Albert 2018) and even offer the opportunity to verify whether some information could be considered "fake news" (Huckle and White 2017). Blockchain has also been considered valuable as a validation mechanism for research, capable of enriching the peer-review process by making data from the published results available (Treadway and van Rossum 2018).

To systematize the blockchain research agenda, Risius and Spohrer (2017) proposed a framework that analyzes technological practices across "groups of activities"

such as "measurement and value" and "management and organization". According to the authors, different "levels of analysis" such as "users and society" and "firms and industry" must be considered for impact assessment. They thus suggest that observing the interplay of multiple stakeholders across different ways of designing and implementing the technology may facilitate the shift from the current state, where general questions are being asked, to a narrower focus on issues that are likely to emerge once blockchain technology becomes pervasive. Multiple perspectives about potential challenges need to be explored, and this chapter hopes to contribute to this effort experimentally.

Challenges of Blockchain

Many of the socio-technical concerns attributed to Bitcoin can shed light on existing concerns about blockchain technology. For example, although many proponents suggest that Bitcoin advances security standards and trust (Subramanian 2018), not knowing who is participating in the network raises concerns about the risk of fraud and crime in the use of the technology (Giungato et al. 2017). We can anticipate that security will continue to be an issue for blockchain implementations to constantly safeguard against (Ouaddah et al. 2016). To Swan (2017), the challenge is finding ways of getting "businesses to explore the new frontier enabled by digital ledgers, while managing an environment that simultaneously invites new kinds of scams and wrongdoing".

In a sense, blockchain and IoT raise similar concerns. Jointly, their challenges may grow even larger. They may include scalability issues (Biswas and Muthukkumarasamy 2016; Zheng et al. 2016), differences in communication standards (Christidis and Devetsikiotis 2016), and the ability to integrate with different technologies like data analytics (Zheng et al. 2016). To Ouaddah et al. (2016), enabling "the application of security and access control mechanisms over constrained environments" is a challenge when delivering IoT services. Leveraging blockchain technology is then challenging due to its inherent complexity both in terms of implementation and its fit with existing business processes (Michelman and Catalini 2017; Swan 2017).

Since it is an incipient topic, there are many research gaps involving blockchain technology that are likely to endure for some time. In particular, however, research suggests that the study of blockchain technology has been specially dedicated to technical aspects and applications (Li et al. 2018; Risius and Spohrer 2017). As research advances, many concerns involving business incentives and stakeholders at different levels, like individuals and organizations from the private and the public sector (Li et al. 2018), may emerge. One could even consider the fact that obstacles have not been studied nearly as much as the opportunities for development as a challenge itself. While interest in blockchain technology seems to be unfolding faster than previous technologies like the Internet (Tapscott and Tapscott 2017), technological euphoria should be combined with healthy levels of skepticism. On top of

the already acknowledged need for more empirical studies, and despite an "unclear development path" (Alcazar 2017), diligent assessment of a new technology tends to be especially important in the early stages, when issues have the chance to be carefully examined before high-stake endeavors involving the larger public start to take place.

Centralization and Exposure to Threats

With the rapid development of information technology, more and more "things"—both physical and virtual—will be connected to networks. According to Gartner (Hung 2017), the number of connections with "things" will be around 20 billion in 2020 and reach 100 billion by 2025. Along with the benefits of interconnectedness, many challenges associated with having centralized networks will also emerge. For example, cloud centers as a current centralized solution for data storage will be under heavy pressure to connect continuously growing amounts of IoT devices, which, as referred before, may catastrophically expose an entire network through a single point.

Many IoT devices are too vulnerable to be trusted (Sicari et al. 2015; Yan et al. 2014). Although often portrayed as a "trust distributed technology" (Olnes et al. 2017), blockchain technology enactment in IoT environments is not immune to threats. In a study that examines the integration of blockchain technology applications and IoT, Dorri et al. (2016) observed that, despite not being able to outmaneuver encryption, threats may still arise in a variety of ways. According to the authors, "adversaries are able to sniff communications, discard transactions, create false transactions and blocks, change or delete data in storage, link a user's transactions to each other and sign fake transactions to legitimize colluding nodes". Researchers say that threats basically belong to three categories: (1) accessibility, (2) anonymity, and (3) authentication and access control. With regard to accessibility, adversaries may, for example, work toward not allowing actual users to access data and services. Risks to anonymity may include systematic efforts to analyze public information and uncover identities. Finally, authentication refers to identity theft as a means of getting access to someone else's data.

Henceforth, threats are not depicted as being necessarily inherent to the functionality of blockchain technology, but to the technological environment where blockchain technology and related technologies operate. Since blockchain technology is expected to integrate with other types of technologies, attacks are also likely to come from peripheral vulnerabilities, or through a distributed denial-of-service (DDoS) attack. These attacks should be of special concern to smart cities, where interconnectedness is a desired feature and the balance between security and technological interoperability is key (Biswas and Muthukkumarasamy 2016; Bou-Harb et al. 2013).

Organizational, Institutional and Political Environments

According to Schlegel et al. (2018), challenges involving blockchain may be technical, institutional, or human. Authors suggest that technical issues may relate to computational power and cost, as observed by Lee and Lee (2017), or the fact that people are not acquainted with the process. Given the multitude of stakeholders involved, the institutional and organizational capacity to adapt to the technology should be taken into consideration (O'Leary 2017). For instance, citizens are expected to benefit from the fact that blockchain may yield more transparency and trust, for instance, in the voting process (Galloway 2017; Marsal-Llacuna and Oliver-Riera 2017); however, research has also considered challenges to its acceptance in states and institutions that are abusive toward their constituents (Hughes 2017). That suggests that the way blockchain technology will be used is context-specific, with laws and regulations playing a role even if those governments are not necessarily opposed to blockchain's technical functionalities (Swan 2017).

It is important to assert that a technology that counts on a decentralized modus operandi should be studied with socio-technical rigor, especially because it may be influenced by political biases (Winner 1980). Velasco (2017), for example, argued that blockchain may carry "political ontologies" to the extent that it displaces the role of traditional institutional actors and dilutes their power and influence. According to the author, these types of incidents are worth monitoring and require mixed ontologies that account for the interplay of technologies and politics. Complementarily, De Filippi and Loveluck (2016) observed that despite the open source nature of the bitcoin project, a limited number of programmers still exert power over how the solution is handled, which echoes several prior studies where ownership over data has been identified as being critical to the expected and actual results (Smolenski 2018b).

It is clear, therefore, that the opportunities and challenges of blockchain technologies are expected to grow in scope and depth. In scope, mainly because of its coexistence with other technologies in a world where ubiquitous computing is, at least tentatively, the norm. Blockchain's peculiarities are likely to emerge more often and more abruptly as the interplay with specific technological conditions and social contexts becomes more evident. For example, blockchain technology is perceived to be an enabler of bitcoin, but more research is needed on the implications of having that approach replicated in contexts other than cryptocurrency (Underwood 2016). Challenges should be carefully considered if blockchain technology is to become a valid framework to address real issues in the public sphere, such as the need to properly manage IoT data in the context of smart cities and other government initiatives. That topic is the focus of our next section.

Using Blockchain Technology to Enhance IoT Data Management

Little research has been dedicated to exploring the relationship between blockchain technology and data management. This section summarizes related work on enhancing IoT data management by using blockchain technology, which includes device management, data access control, identity management, and data storage, among others.

Data management is the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information assets.[1] One IDC study has focused on the relationship between blockchain and data management (see Bond 2017). Blockchain technology has already been tested for data sharing in clinical research (Benchoufi and Ravaud 2017) and intelligent vehicles (Singh and Kim 2017), and has shown big potential for building trust, preserving privacy, and enhancing security (Park and Park 2017). It is also believed to benefit supply chain management ("The Benefits of Blockchain to Supply Chain Networks" 2017), in which it could establish a shared, secure record of information flows. This is similar to a "shared version of events" across networks for supply chain transactions, processes, and partners, to the extent that it enables improved supply chain efficiencies, better multiparty collaboration, and streamlined processes for dispute resolution.

In studying the combination of blockchain and IoT, Christidis and Devetsikiotis (2016) examine what a blockchain is, how it operates, and how smart contracts automate interactions between transaction parties. The authors highlight issues from transactional privacy concerns to the expected value of the digitized assets when traded on the network. Since IoT applications and platforms' reliance on a centralized cloud are certainly a concern from a security standpoint, blockchain-based identity and access management systems, such as those associated with IP spoofing, can be leveraged to strengthen IoT security (Kshetri 2017a).

For IoT data management, access control and protection are big issues, especially for private and sensitive data such as medical records, which are collected with more and more IoT devices. Zhang et al. (2018) focus on addressing the access control issue of IoT. They propose a smart contract-based framework to achieve distributed and trustworthy access control for IoT systems. For data access protection, a smart contract system (a set of smart contracts) is designed and implemented where access control methods can be registered, updated, and deleted.

A framework—FairAccess—has been proposed based on blockchain technology (Ouaddah et al. 2016, 2017). In that endeavor, researchers propose a novel distributed privacy preserving authorization management system that manages access control on behalf of constrained devices. In the framework, the smart contract is

[1] https://technicspub.com/dmbok/

also being used to express fine-grained and contextual access control policies to make authorization decisions. Since the data management principles are maintained, no one could be systematically forced to lose control over her or his own data; each node in the network shares the data with others directly, without the intervention of any third or trusted party. Importantly, the framework has leveraged the so-often referenced consistency offered by blockchain-based cryptocurrencies such as bitcoin to provide a stronger and more transparent access control tool.

With a focus on medical data management, Azaria et al. (2016) proposed MedRec, a blockchain-based way of addressing problems related to medical data sharing and system interoperability. It sets out to do so by implementing permission mechanisms and data integrity logic on-chain to support medical stakeholders with record authenticity, auditability and data sharing. That approach could potentially improve data quality and enhance data volume for medical research. Targeting privacy protection, Ali et al. (2017) consider IoT a distributed data storage system named IPFS (Interplanetary File System) (Labs 2018). IPFS is referred to as the "Distributed Web" or a "peer-to-peer hypermedia protocol to make the web faster, safer, and more open" (Labs 2018). By defining a "content-addressed file system", it features "block-level deduplication" and uses crypto approaches that ensure file integrity and versioning (Labs 2018). In this approach, IoT data can be grouped and stored in IPFS, while the blockchain only needs to hold the hash of the IPFS files containing the IoT data.

As per some of the cases presented above, blockchain technologies open a promising path for data management with several stakeholders. Through them, smart contracts can be flexibly designed to implement data management policies. In light of the blockchain initiatives presented, this chapter will explore one blockchain application from a different angle. Taking IoT data management and utilization as a case study, the goal is to examine blockchain technology adoption in the context of data governance in the public sector. Data governance is the overall management of the availability, usability, integrity, and security of data. A sound data governance program includes a governing body or council, a defined set of procedures, and a plan to execute those procedures, by definition published by TechTarget.[2]

For the experiments, we built a very small IoT system to simulate data production and management, and combined it with blockchain technology, so as to explore the benefits of blockchain technology to enhance IoT data management and better understand how they would work together. This proposed framework is discussed in detail in the following section.

[2] https://searchdatamanagement.techtarget.com/definition/data-governance

Proposing a Case Study and a Conceptual Experiment

This section presents the case we used to test the ideas proposed in this chapter. In our experiments, an IoT network was built, a private blockchain based on Ethereum was set up, and they were then combined. Finally, a set of smart contracts for managing IoT data with different policies was proposed, implemented, and tested.

As a decentralized technology, blockchain can be used for any transaction or information exchange that happens in government, including digital identity, e-voting, and criminal records, among others. In this chapter, we take IoT data management as a case to study the potential benefits and challenges in the public sector for smart city initiatives. The idea of the case study presented in this paper was to develop an IoT simulation platform combined with a blockchain network. The goal was to investigate how IoT data governance can benefit from blockchain technology and smart contracts, particularly with regard to receiving, storing, integrating, and allowing for exchange or utilization of data from IoT devices. As described above, Christidis and Devetsikiotis (2016) provided an overview of blockchains and smart contracts for IoT and examined issues related to them. However, the authors do not address any issues related to the management of IoT data. This chapter explores this gap by building a simulation environment that explores what blockchain technology can do for IoT data management. We built an IoT ecosystem to simulate data production, transfer, sharing, and use, which is a simulated application scenario similar to potential government uses. The goal is to theoretically identify issues that likely need to be tackled in practice.

For the experiment, we followed a series of steps. First, we set up an IoT network, which included (a) a data producer; (b) a data consumer, and (c) a data carrier as parts of the IoT ecosystem. Second, we established a private blockchain with several nodes, each with its own account and the ability to communicate with each other. Third, and most importantly for this study, IoT data was integrated with blockchain. That means that data from IoT devices was stored in a private blockchain. In this experiment, blockchain worked as a database for IoT devices where smart contracts should be designed and implemented to enhance data management. Lastly, data could be retrieved from the blockchain flexibly for further utilization, for example, developing a data visualization application.

Examining Smart Contracts Through Ethereum

Smart contracts are codes implemented on the blockchain for managing interactions between nodes and participants of the system based on data. They can have conditions and consequences depending on actions. A smart contract usually provides many functions or application binary interfaces (ABIs) that can be used to interact with it. Triggering a smart contract is done by addressing a transaction from an

account or a message from another contract to it. It can also be executed by invoking the call function without sending transactions and messages (Zhang et al. 2018).

As described, smart contracts are good ways to interact with blockchain data. Ethereum ("Ethereum Project" 2018) was chosen as the blockchain platform to conduct the simulation. Just as in bitcoin, Ethereum also has a blockchain containing blocks of transactions in which a consensus has to be reached by all the nodes connected to the network. This is consistent with what is known about blockchain technology; each node can have a copy of the whole blockchain. Moreover, Ethereum provides a decentralized turing-complete virtual machine (Wang 2017), called the Ethereum Virtual Machine (or EVM for short). That means that EVM can run any computer program one defines and is powerful enough to implement any program in any similarly computationally complete system (Wang 2017).

Ethereum allows developers to program their own smart contracts and define EVM instructions. These smart contracts can be written using friendly programming languages like Solidity ("Solidity 0.4.20 documentation" 2018), which is a Java script-like language developed specifically for writing smart contracts. The smart contract is run by each of the nodes in the network, which maintain and alter states within the database. To run smart contracts on the Ethereum platform, you need to pay for it, and the payment (or fee) is calculated in Ether (ETH) via an intermediary benchmark called "gas limit" and "gas price". Ether is the name of the currency used within Ethereum, and it is used to pay for computation within the EVM. To obtain Ether, one needs to either become an Ethereum miner or trade other currencies for it.

In the simulation, Ethereum's smart contracts were used to create intelligent and automatic policies to manage the data. The framework is shown in Fig. 1. The system was designed to implement contracts to store, integrate, exchange, and get data for client utilization. For example, IoT sensors produce temperature and humidity readings every second. To make data more useful and accessible in the future, storing temperature and humidity with a timestamp as well as some form of the unique IoT device ID would be recommended.

As shown in Fig. 2, one temperature sensor and one humidity sensor were used as two IoT devices to capture (or produce) data. Due to their computing capability,

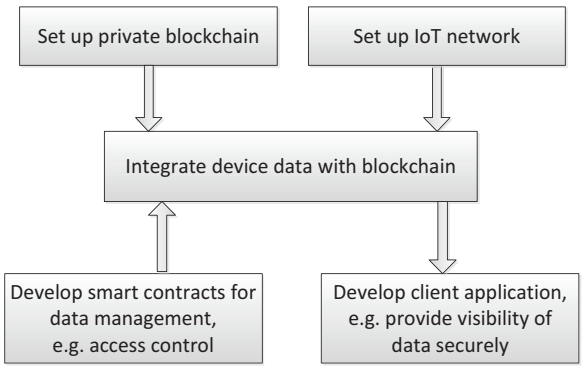


Fig. 1 Diagram of experimental framework

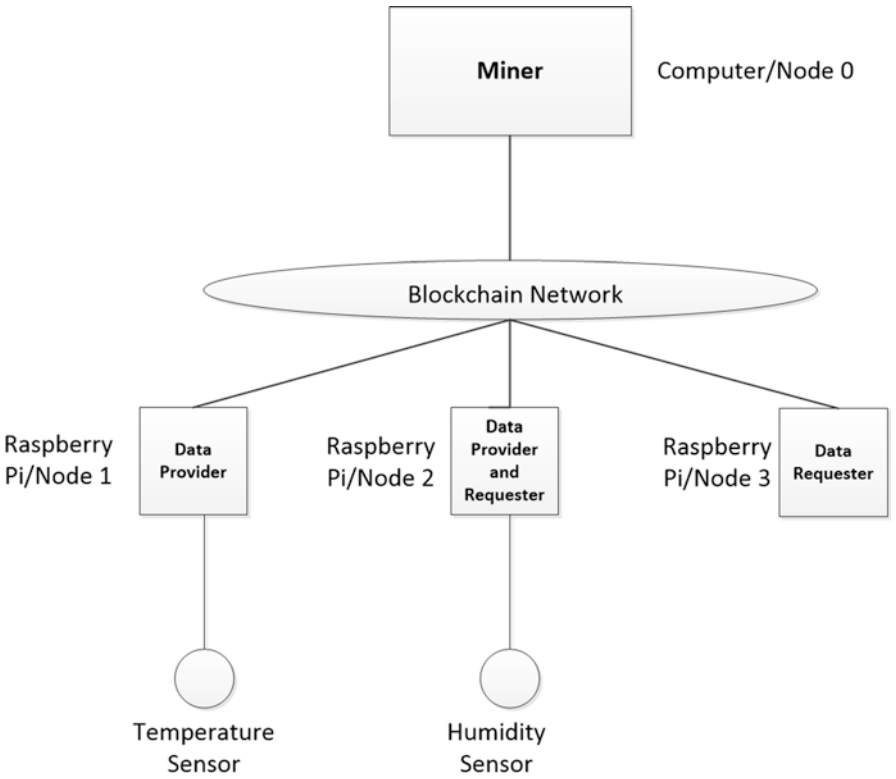


Fig. 2 IoT data scenario

both sensors needed a Raspberry Pi (RPi) as a proxy to connect to the blockchain network to store or capture data. Essentially, RPis were installed in an Ethereum client and worked as a "data carrier" node. A separate RPi was also connected to the blockchain that would only work as a data requester to play the specific role in our simulation.

As described above, running smart contracts or completing transactions on Ethereum blockchain costs gas, which, in turn, costs Ether (ETH). RPis do not have enough computing and storage resources to generate ETH. Therefore, one laptop in the experiment was also connected to the network, working as a miner for producing ETH. Through this private blockchain network created based on Ethereum, it became possible to enable the experiment by generating the ETH as needed.

We implemented several smart contracts for IoT data management to show their potential when combined with blockchain (Fig. 3). For Smart Contract A, only the IoT device that deploys the contract could get its data after being stored on the blockchain (Fig. 4). For B, the IoT device that deploys the contract could authorize another node to retrieve the data being stored on the blockchain (Fig. 5). For C, all the data stored on the blockchain could be captured and utilized by a third party, which would mean the data was open to the public (Fig. 6).

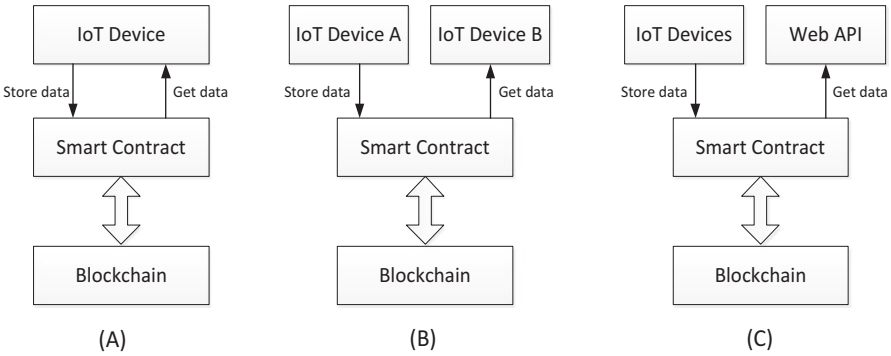


Fig. 3 Smart contracts-based data management

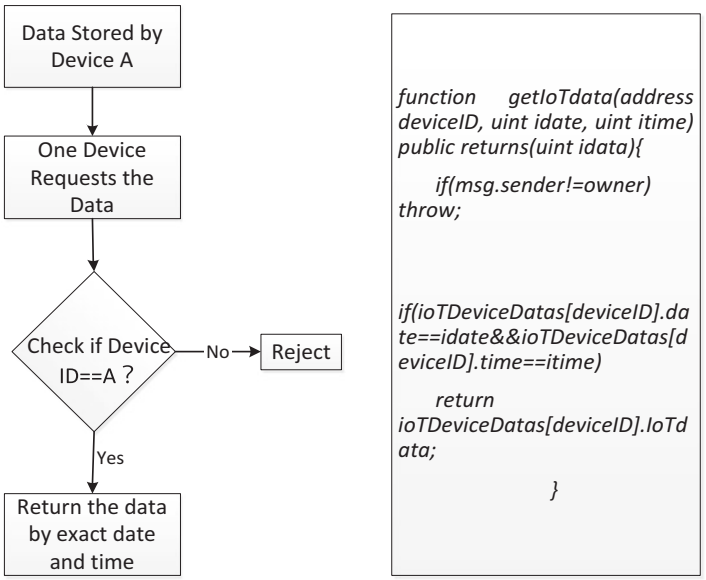
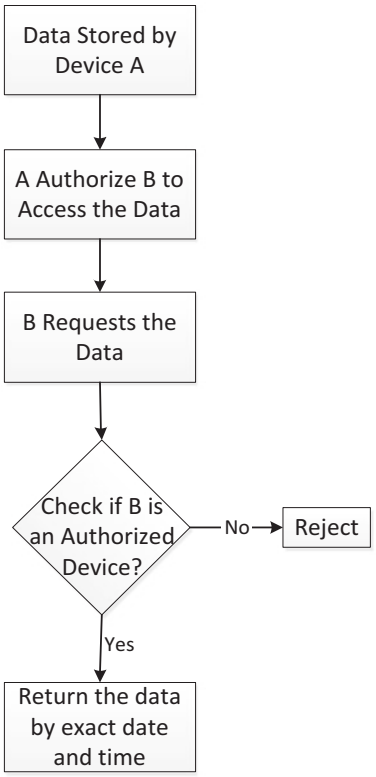


Fig. 4 The pseudo code of Smart Contract A

The basic smart contract for storing IoT data is depicted in Fig. 7, which is also shown in the pseudo code. There, the structure of the IoT data (including date and time as the timestamp) is defined and the IoT device ID is used as the reference of the data array. All of them were later used as the key to finding the exact data being requested and queried.

It is worth mentioning that all of the above smart contracts run based on a blockchain network. That means that the data managed by the smart contracts benefit from blockchain technology attributes, such as being decentralized and being



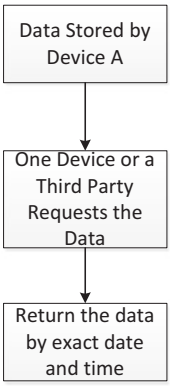

```
address public admin;
function isAdmin() constant returns (bool){
    return msg.sender == admin;
}

function setAdmin(address addr) constant returns (bool){
    if(isAdmin()){
        admin=addr;
        return ture;
    }
    return false;
}
function getIoTdata(address deviceID, uint idate, uint itime) public returns(uint idata){
    if(msg.sender!=admin) throw;

if(ioTDeviceDatas[deviceID].date==idate&&ioTDeviceDatas[deviceID].time==itime)
    return ioTDeviceDatas[deviceID].IoTdata;
}
```

Fig. 5 The pseudocode of Smart Contract B

Fig. 6 The pseudocode of Smart Contract C




```
function getIoTdata(address deviceID, uint idate, uint itime) public returns(uint idata){

if(ioTDeviceDatas[deviceID].date==idate&&ioTDeviceDatas[deviceID].time==itime)
    return ioTDeviceDatas[deviceID].IoTdata;
}
```

Fig. 7 The pseudocode of smart contract for storing data

```
contract StoreAndGetIoTdata{

    struct IoTDeviceData{
      uint IoTdata;
      uint date;
      uint time;
    }

    mapping(address=>IoTDeviceData) public ioTDeviceDatas;

    function storeIoTdata(address deviceID, uint idate, uint
itime, uint idata){
    ioTDeviceDatas[deviceID].IoTdata=idata;
    ioTDeviceDatas[deviceID].date=idate;
    ioTDeviceDatas[deviceID].time=itime;
    }
}
```

protected against tampering or tracing. When a smart contract is deployed on a blockchain, it will have an account address, which is the same as an Ethereum node. Thus, the nodes belong to the blockchain network and could communicate with the smart contract through its address. In theory, one could develop as many smart contracts as needed, as long as the expense of running them on the blockchain can be afforded. However, in practice, the problem is that it could not be modified or destroyed once the smart contract is deployed.

Discussion and Implications

This section discusses the technical implementation challenges involved in the process, explains how the simulation conducted in the chapter is related to data sharing and management in the public sector, and what needs to be considered when implementing smart contracts in practice.

The experimental procedures described in this chapter as a workflow diagram shed light on some important considerations. The discussion in this chapter focuses on the benefits of applying blockchain technology to the governance of IoT data and the technical implementation challenges involved in the process. While benefits include both data security protection and multisource data management and usage, challenges include the storage of distributed data and the design and implementation of flexible data governance strategies.

Blockchain shows great potential across a wide range of business and government applications. As the literature suggests, blockchain is expected to impact multiple fields, including finance, accounting, healthcare, manufacturing, insurance, retail, law, and government. It is also reasonable to expect that applications will be developed at the intersection of those fields and many others. Such socio-technical innovations deserve further scrutiny because domains like government, in which the smart cities movement receives large attention, are likely to be particularly sensitive to institutional, organizational, and political dynamics. Therefore, it seems clear that IoT and blockchain working together could generate important benefits for smart cities and other public-sector initiatives.

There is some escalating consensus that blockchain can help establish trust, accountability, transparency, and efficiency while streamlining processes. As exposed in the early sections of this chapter, one of the biggest issues with IoT data is security. Concerns are not only related to keeping track of the data from the very beginning to guarantee it is from a trusted source but also about how to control access to the data. The basis of a blockchain-enabled network is to provide crypto-based access control that is peer-to-peer in its implementation. A blockchain enables devices to register directly to the network. Also, each identity can be associated with the device's public key, thus enabling more security and trust in the overall network.

As a decentralized distributed storage technology, blockchain benefits IoT data management in the following ways. First, due to decentralization, no centralized organization or node can fully master the data, which can reduce data leaks or data monopolies. Second, through distributed storage, data has multiple backups; single node damage does not affect the rest of the data. Encrypted, tamperproof storage also increases data security. More importantly, through smart contracts, flexible data access control policies can be implemented, data rights can be better distributed, and multisource data can be integrated and shared in a decentralized manner.

In Ethereum, everything stored to a contract costs gas or ETH. For IoT data, the continuous production could prove very expensive. Although that constraint was not taken into consideration in the experiment, mitigating some of the costs by storing some data off-chain with a decentralized storage system like IPFS could be advisable.

In the simulation, three Raspberry Pi (RPi) nodes were connected to the blockchain network; one node worked as a data provider, one node as both a data provider and requester, and one only as a data requester. By simulating different roles being played, this scenario is similar to three parties or agencies who want to share their data in the public sector, especially in an untrusted environment. That suggests that they all need different roles and permissions to maintain their data rights and preserve security, as well as to ensure that the data exchange has a traceable record.

Despite being a simple case study in data governance, it is clear that smart contracts operate under strict rules; hence, they require negotiation and consensus between different stakeholders in practice, with every smart contract designed and implemented cautiously. Extensions of the blockchain technology-based IoT data management framework presented in this chapter could also be considered for applications in local governments that engage in smart cities initiatives with

IoT. Nonetheless, considering the policy context and the extent to which stakeholders will be involved in "smart contracting" is critical. Besides not being a technological problem alone, blockchain should be thought of and designed through the lenses of smart contractors and their levels of participation in this process. Only then can high levels of transparency and security and low levels of risk be ensured for citizens.

Conclusion

This study found that blockchain technology provides a decentralized way to manage IoT data, which implies greater security because it is distributed, tamperproof, and traceable. In addition, smart contracts could also be flexibly designed and implemented to achieve different data management policies, which is particularly important in complex interorganizational environments such as policy networks and service-delivery government programs.

IoT is a way to realize the digitization of the physical world and a foundational part of what is known as a smart city. IoT data, in particular, enable the smart city vision by allowing for the collection, storage, integration, analysis, and mining of great volumes of data to produce a variety of intelligent applications, data products, and services. All those processes are expected to aid decision-making, increase efficiency, improve services, and benefit citizens.

Furthermore, as outlined in this chapter, blockchain technology may play a complementary role in IoT data management. As an emerging, decentralized, and distributed ledger technology, blockchain offers a promising avenue to address many shortcomings in the conventional centralized IoT data system because it provides a safer and more efficient way to store, manage, and use data for IoT. That is critical because, in the context of smart cities, privacy and security are a concern for IoT data management, involving issues such as knowing who has the data rights, who can access the data, and how the data should be stored.

This chapter proposes a conceptual framework and a technical experiment in which blockchain is proposed to enhance IoT data management and explore the potential of this technology to benefit data governance in the public sector. The case study shows that aside from the advantages that blockchain provides, smart contracts could also be flexibly designed and implemented to achieve different data management policies, a condition that is critical to complex interorganizational environments in the public sector.

Finally, it cannot be emphasized enough that to a certain extent blockchain technology's disruption in government is already happening, and not without implications and controversies regarding governance. Despite expectations for greater transparency in data manipulation, opportunities for blockchain implementation have been portrayed as being very context-specific. Moving forward, enacting blockchain requires us to consider some factors that have not been extensively mapped regarding domain and scope, a step that should occur despite blockchain's

apparent tendency of morphing into a general purpose technology (Allen 2017). While the process of mapping determinants and risks seems to be underway, theorizing efforts should continue to be followed by experimental approaches, empirical studies, and reports of the lessons learned from them, particularly in the context of smart city applications using sensors and other IoT devices with limited security, performance, and storage capabilities.

References

Adams, R., Parry, G., Godsiff, P., & Ward, P. (2017). The future of money and further applications of the blockchain. *Strategic Change-Briefings in Entrepreneurial Finance, 26*(5), 417–422. https://doi.org/10.1002/jsc.2141.

Ali, M. S., Dolui, K., & Antonelli, F. (2017, October). IoT data privacy via blockchains and IPFS. In Proceedings of the Seventh International Conference on the Internet of Things (p. 14). ACM.

Alcazar, V. (2017). Data you can trust: Blockchain technology. *Air & Space Power Journal, 31*(2), 91–101.

Allen, D. W. (2017). Blockchain innovation commons. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2919170.

Anh, D. T. T., Zhang, M., Ooi, B. C., & Chen, G. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering, 30*, 1366–1385.

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *Computer (00189162), 50*(9), 18–28. https://doi.org/10.1109/MC.2017.3571064.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *International Conference on Open and Big Data (OBD)* (pp. 25–30). New York: IEEE.

Ban, H. J., Choi, J., & Kang, N. (2016). Fine-grained support of security services for resource constrained Internet of Things. *International Journal of Distributed Sensor Networks, 12*, 1–8. https://doi.org/10.1155/2016/7824686.

Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials, 18*(1), 335.

Biswas, K., & Muthukkumarasamy, V. (2016). *Securing smart cities using blockchain technology* (J. Chen & L. T. Yang, Eds.). New York: IEEE.

Bjerg, O. (2016). How is bitcoin money? *Theory, Culture & Society, 33*(1), 53–72.

Bond, S. (2017). *Blockchain—A data management, integration, and integrity disruptor?* Retrieved February 27, 2018, from http://www.idc.com/getdoc.jsp?containerId=US42074217.

Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2014). Fog computing: A platform for internet of things and analytics. In *Big data and internet of things: A roadmap for smart environments* (pp. 169–186). Basel: Springer.

Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M., & Assi, C. (2013). Communication security for smart grid distribution networks. *IEEE Communications Magazine, 51*(1), 42–49. https://doi.org/10.1109/MCOM.2013.6400437.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper*.

Carlozo, L. (2017). What is blockchain? *Journal of Accountancy, 224*(1), 1–2.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339.

Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on blockchain: Costs savings thanks to the blockchain technology. *Future Internet, 9*(3), 25. https://doi.org/10.3390/fi9030025.

Dalčeković, N., Vukmirović, S., Stoja, S., & Milošević, N. (2017). Enabling the IoT paradigm through multi-tenancy supported by scalable data acquisition layer. *Annals of Telecommunications, 72*(1–2), 71–78.

De Filippi, P., & Loveluck, B. (2016). The invisible politics of Bitcoin: Governance crisis of a decentralised infrastructure. *Internet Policy Review, 5*(3). https://doi.org/10.14763/2016.3.427.

Debabrata, G., & Albert, T. (2018). A framework for implementing blockchain technologies to improve supply chain performance. *SCALE Working Paper Series*.

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science, 5*(2), 121–147.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering, 19*(5), 92–95.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: Challenges and solutions. *arXiv Preprint arXiv:1608.05187*.

Eldred, M. (2016). Blockchain thinking and euphoric hubris (vol 35, pg 39, 2016). *IEEE Technology and Society Magazine, 35*(2), 27–27.

Ethereum Project. (2018). Retrieved March 3, 2018, from https://www.ethereum.org/.

Galloway, K. (2017). Digital solutions to political reform. *Eureka Street, 27*(7), 24–26.

Gil-Garcia, J. R., Helbig, N., & Ojo, A. (2014). Being smart: Emerging technologies and innovation in the public sector. *Government Information Quarterly, 31*(Supplement 1), 11–18. https://doi.org/10.1016/j.giq.2014.09.001.

Giungato, P., Rana, R., Tarabella, A., & Tricase, C. (2017). Current trends in sustainability of bitcoins and related blockchain technology. *Sustainability, 9*(12), 2214. https://doi.org/10.3390/su9122214.

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. *Hawaii International Conference on System Sciences*.

Huckle, S., & White, M. (2017). Fake news: A technological approach to proving the origins of content, using blockchains. *Big Data, 5*(4), 356–371. https://doi.org/10.1089/big.2017.0071.

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. *Procedia Computer Science, 98*, 461–466.

Hughes, K. (2017). Blockchain, the greater good, and human and civil rights. *Metaphilosophy, 48*(5), 654–665. https://doi.org/10.1111/meta.12271.

Hung, M. (2017). *Leading the IoT*. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

Ibba, S., Pinna, A., Seu, M., & Pani, F. E. (2017). CitySense: Blockchain-oriented smart cities. In *Proceedings of the XP2017 Scientific Workshops* (p. 12). New York: ACM.

Koh, J. M., Sak, M., Tan, H.-X., Liang, H., Folianto, F., & Quek, T. (2015). Efficient data retrieval for large-scale smart city applications through applied Bayesian inference. In *2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)* (pp. 1–6). https://doi.org/10.1109/ISSNIP.2015.7106930.

Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications, 9*(2), 397–413. https://doi.org/10.1007/s12083-015-0347-x.

Kshetri, N. (2017a). Can blockchain strengthen the Internet of Things? *IT Professional, 19*(4), 68–72. https://doi.org/10.1109/MITP.2017.3051335.

Kshetri, N. (2017b). Potential roles of blockchain in fighting poverty and reducing financial exclusion in the global south. *Journal of Global Information Technology Management, 20*(4), 201–204. https://doi.org/10.1080/1097198X.2017.1391370.

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068.

Labs, P. (2018). *IPFS is the distributed Web*. Retrieved March 1, 2018, from https://ipfs.io/.

Lee, B., & Lee, J.-H. (2017). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *Journal of Supercomputing, 73*(3), 1152–1167. https://doi.org/10.1007/s11227-016-1870-0.

Li, Y., Marier-Bienvenue, T., Perron-Brault, A., Wang, X., & Paré, G. (2018). Blockchain technology in business organizations: A scoping review. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Marsal-Llacuna, M.-L., & Oliver-Riera, M. (2017). The standards revolution: Who will first put this new kid on the blockchain? In *ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)* (pp. 1–7). New York: IEEE.

Marsal-Llacuna, M. L. (2018). Future living framework: Is blockchain the next enabling network?. Technological Forecasting and Social Change, 128, 226–234. Chicago

Meijer, A. J., Gil-Garcia, J. R., & Bolívar, M. P. R. (2016). Smart city research: Contextual conditions, governance models, and public value assessment. *Social Science Computer Review, 34*(6), 647–656.

Michelman, P., & Catalini, C. (2017). Seeing beyond the blockchain hype. *MIT Sloan Management Review, 58*(4), 17–22.

Nguyen, Q. K. (2016). *Blockchain—A financial technology for future sustainable development*. New York: IEEE.

O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intelligent Systems in Accounting Finance & Management, 24*(4), 138–147. https://doi.org/10.1002/isaf.1417.

Olnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007.

Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science, 11*(4), 404–428.

Ouaddah, A., Abou Elkalam, A., & Ouahman, A. A. (2016). FairAccess: A new blockchain-based access control framework for the Internet of Things. *Security and Communication Networks, 9*(18), 5943–5964. https://doi.org/10.1002/sec.1748.

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In *Europe and MENA Cooperation advances in information and communication technologies* (pp. 523–533). Berlin: Springer.

Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry (20738994), 9*(8), 1–13. https://doi.org/10.3390/sym9080164.

Porru, S., Pinna, A., Marchesi, M., & Tonelli, R. (2017). Blockchain-oriented software engineering: Challenges and new directions. In *Proceedings of the 39th International Conference on Software Engineering Companion* (pp. 169–171). New York: IEEE Press.

Potts, J., Rennie, E., & Goldenfein, J. (2017). Blockchains and the crypto city. *IT-Information Technology, 59*(6), 285–293. https://doi.org/10.1515/itit-2017-0006.

Rahim, S. R. M., Mohamad, Z. Z., Bakar, J. A., Mohsin, F. H., & Isa, N. M. (2018). Artificial intelligence, smart contract and Islamic finance. *Asian Social Science, 14*(2), 145.

Ranjithprabhu, K., & Sasirega, D. (2014). Eliminating single point of failure and data loss in cloud computing. *International Journal of Science and Research, 3*(4), 2319–7064.

Rathore, M. M., Ahmad, A., Paul, A., & Rho, S. (2016). Urban planning and building smart cities based on the internet of things using big data analytics. *Computer Networks, 101*, 63–80.

Risius, M., & Spohrer, K. (2017). A blockchain research framework what we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering, 59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0.

Rosas, J., Brito, V., Palma, L. B., & Barata, J. (2017). Approach to adapt a legacy manufacturing system into the IoT paradigm. *International Journal of Interactive Mobile Technologies, 11*(5), 91–104.

Schlegel, M., Zavolokina, L., & Schwabe, G. (2018). Blockchain technologies from the consumers' perspective: What is there and why should who care? In *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.

Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy, 195*, 234–246. https://doi.org/10.1016/j.apenergy.2017.03.039.

Singh, M., & Kim, S. (2017). Blockchain based intelligent vehicle data sharing framework. *arXiv Preprint arXiv:1708.09721*.

Smolenski, N. (2018a). The evolution of trust. *Scientific American, 318*(1), 38–41.

Smolenski, N. (2018b). The evolution of trust the ultimate social impact of blockchain technology depends on who controls our digital identities. *Scientific American, 318*(1), 38–41.

Solidity—Solidity 0.4.20 documentation. (2018). Retrieved March 7, 2018, from https://solidity.readthedocs.io/en/v0.4.20/.

Subramanian, H. (2018). Decentralized blockchain-based electronic marketplaces. *Communications of the ACM, 61*(1), 78–84. https://doi.org/10.1145/3158333.

Swan, M. (2015). Blockchain thinking: The brain as a decentralized autonomous corporation [Commentary]. *IEEE Technology & Society Magazine, 34*(4), 41–52. https://doi.org/10.1109/MTS.2015.2494358.

Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology Innovation Management Review, 7*(10), 6–13. https://doi.org/10.22215/timreview/1109.

Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review, 58*(2), 10–13.

The Benefits of Blockchain to Supply Chain Networks. (2017, October 25). Retrieved February 27, 2018, from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZZO12537USEN.

Treadway, J., & van Rossum, J. (2018). What is blockchain for research? *Research Information, 94*, 12–13.

Underwood, S. (2016). Blockchain beyond Bitcoin. *Communications of the ACM, 59*(11), 15–17. https://doi.org/10.1145/2994581.

Velasco, P. R. (2017). Computing ledgers and the political ontology of the blockchain. *Metaphilosophy, 48*(5), 712–726. https://doi.org/10.1111/meta.12274.

Wang, K. (2017, July 10). *Ethereum: Turing-completeness and rich statefulness explained*. Retrieved March 9, 2018, from https://hackernoon.com/ethereum-turing-completeness-and-rich-statefulness-explained-e650db7fc1fb.

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*, 121–136.

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, 42*, 120–134.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal, 6*(2), 1594–1605.

Zheng, Z., Xie, S., Dai, H.-N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.

Lingjun Fan received his PhD degree in computer architecture from University of Chinese Academy of Sciences. Currently, he is a research director of Information Technology Strategy Research Center at Institute of Computing Technology, Chinese Academy of Sciences, and a visiting scholar in Center for Technology in Government, UAlbany, SUNY. His research interests include information technology development trends, smart city, big data, Internet of Things, blockchain technology, and so on. He is currently undertaking a sub-project from National Science Foundation of China on governing government big data. A special research interest is focused on

using blockchain technology to manage and share government big data. Lingjun Fan has published more than 30 papers in journals and conferences proceedings, including People's Daily, Global Times, Big Data, and obtained a best paper award in the HPC China 2012.

Felippe Cronemberger received his PhD in information science from the College of Emergency Preparedness, Homeland Security and Cybersecurity at University at Albany, State University of New York. He worked as a research assistant at the Center for Technology in Government through the SUNY Research Foundation and was a visiting research fellow at Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University) in Russia, where he supported research on smart cities governance. Felippe has worked in education, human resources, consulting, and technology during the past 15 years and his research interests are business and government intelligence, smart cities, and computational social science.

J. Ramon Gil-Garcia is an Associate Professor of Public Administration and Policy and the Research Director of the Center for Technology in Government, University at Albany, SUNY. Dr. Gil-Garcia is a member of the Mexican Academy of Sciences and of the Mexican National System of Researchers. In 2009, he was considered the most prolific author in the field of digital government research worldwide and in 2013 he was selected for the Research Award, which is "the highest distinction given annually by the Mexican Academy of Sciences to outstanding young researchers." Currently, he is also a professor of the Business School at Universidad de las Americas Puebla in Mexico. Dr. Gil-Garcia is the author or co-author of articles in prestigious international journals in Public Administration, Information Systems, and Digital Government and some of his publications are among the most cited in the field of digital government research worldwide.

Part II
Applications, Cases, and Experiences of Internet of Things (IoT) in the Public Sector

Awareness and Smart City Implementations: Sensing, Sensors, and the IoT in the Public Sector

H. Patricia McKenna

Abstract This chapter explores implementation challenges as opportunities for moving beyond smart and connected governments by focusing on awareness in relation to sensing, sensors, and the Internet of Things (IoT) in the public sector in the context of smart cities. A review of the research literature for smart city implementations is conducted from multiple perspectives, highlighting a range of issues and challenges for the public sector. The theoretical framework for this chapter uses the construct of awareness in relation to the key smart city characteristics of adaptability, complexity, innovation, and readiness. The research design for this work utilizes a single case study approach to explore evolving understandings of smart city implementations in contemporary urban environments. Multiple methods of data collection are used including survey and interview while content analysis is used in the iterative analysis of data. Data were collected and analyzed from diverse individuals in multiple small- to medium- to large-sized cities, mostly in Canada and extending to other countries (e.g., Israel). This work makes several contributions by providing (a) an expanded way of looking at IT (information technology) implementation in the public sector for twenty-first century urban environments encompassing sensing, sensors, and the IoT; (b) understandings of IT implementation challenges as opportunities in the public sector for more responsive and aware solution-making; and (c) a conceptual framework for more dynamic notions of implementation in the public sector, as in ambient implementation. This chapter advances an awareness-based explanatory model for ambient implementation of use to the public sector in smart cities.

Keywords eGovernment · Implementation · IoT · Public sector · Sensing · Sensors · Smart cities

H. P. McKenna (✉)
AmbientEase and the UrbanitiesLab, Victoria, BC, Canada

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_6

Abbreviations

AI	Artificial intelligence
BIS	Body insight scale (formerly body intelligence scale)
DG	Digital government
DR	Demand response
DV	Dependent variables
eGovernment	Electronic government
eServices	Electronic services
EA	Enterprise architecture
ES	Electronic services
ESI	Electronic services implementation
HI	Human insights
HRL	Human readiness levels
ICT	Information and communication technology
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IT	Information technology
ITU	International Telecommunications Union
IV	Independent variables
PM	Public management
SCC	Smart Cities Council
web-GIS	Web-based geographic information system

Introduction

This chapter explores implementation challenges as opportunities for moving beyond smart and connected governments by focusing on awareness in relation to sensing, sensors, and the Internet of Things (IoT) in the public sector in the context of smart cities. This work argues that sensing, sensors, and the IoT refer to aware technologies that pose particular implementation challenges for the public sector along with opportunities for rethinking existing understandings of implementation. As such, this work explores understandings at the urban level when people become more aware of their sensing capabilities and of sensor technologies and the IoT as enablers and enhancers of smartness in the public sector and in the public realm in everyday urban spaces. The purpose of this chapter is to explore and shed light on new, more dynamic and adaptive understandings of implementation in contemporary urban contexts, as in ambient implementation, enabled and influenced by aware people and aware technologies. A review of the research literature for smart city implementations is conducted from multiple perspectives highlighting a range of issues and challenges for the public sector. The theoretical framework for this chapter uses the construct of awareness, along with learning, openness, and engagement

as sub-constructs, in relation to the key smart city characteristics of adaptability, complexity, innovation, and readiness. This theoretical perspective and framing enables the conceptualizing of an adaptive implementation framework for operationalizing this exploration of public sector sensing, sensors, and the IoT.

The research design for this work utilizes a single case study approach to explore evolving understandings of the smart city implementation phenomenon in contemporary urban environments through the lens of awareness in relation to sensing, sensors, and the IoT in the public sector. Multiple methods of data collection are used including survey and interview, while content analysis, pattern matching, explanation building, and descriptive statistics are used in the iterative analysis of data. Initial steps are taken toward defining variables for the building of an explanatory model for understanding implementation challenges as opportunities in moving toward smarter public sector environments. Data were collected and analyzed from diverse individuals in multiple small- to medium- to large-sized cities, mostly in Canada and extending to other countries (e.g., Israel). Additional research design details for this work are presented in section "Methodology".

This work makes several contributions by providing (a) an expanded way of looking at information technology (IT) implementation in the public sector for twenty-first century urban environments from an awareness perspective encompassing sensing, sensors, and the IoT; (b) understandings of IT implementation challenges as opportunities in the public sector for more responsive and aware solution-making; and (c) a conceptual framework for more dynamic notions of implementation in the public sector, as in ambient implementation. Practical implications for the value of awareness associated with sensing, sensors, and the IoT in the public sector are identified and recommendations for research directions going forward are outlined in the context of smart cities.

This chapter is included in the current volume because it provides an exploration of the more dynamic, adaptive, and responsive nature of implementation challenges as opportunities for the public sector associated with sensing, sensors, and the IoT as aware technologies involving more aware people. As such, this chapter is particularly relevant to the subject of the current volume in shedding light on public sector sensing, sensors, and IoT implementations in urban contexts as a socio-technical phenomenon while building an awareness-based explanatory model for ambient implementation.

Nam and Pardo (2011) articulated the smart cities concept as a way for cities to innovate themselves through public sector use of information and communication technology (ICT). Charoubi et al. (2012) shed light on the rationale for smart cities, pointing to the unprecedented challenges for the public sector associated with rapid urban growth in the twenty-first century. Konomi and Roussos (2017) observed that "we are now going beyond the last decade's conception of smart cities" and moving "towards a deeper level of symbiosis among smart citizens, Internet of Things and ambient spaces." Schmitt (2017) describes the evolution of smart cities as a movement toward responsive cities where smarter public sector governance recognizes the importance of citizen involvement in the use of smart technologies as part of the planning, design, and management of cities and urban regions.

Based on this background and context, three key elements serving to motivate this work include (a) the nature of sensor and IoT technologies (Scholl 2016); (b) the gap in implementation theorizing for electronic services (El-Haddadeh et al. 2013) such as sensor and IoT technologies in the public sector; and (c) the gap in theoretical frameworks for the responsive city (Hoffman 2016). For example, Scholl (2016) claims that through the Internet of Things (IoT) a kind of smartness is emerging with self-monitoring, directing, and steering capabilities circumscribed by predefined boundaries with a reach to all human activity and transactions with implications for smart governance, government, and cities. El-Haddadeh et al. (2013) refer to the dynamic nature of technologies, pointing to a gap in the research literature related to an undertheorizing of implementation and associated complexities of electronic services (ES) in the public sector. Also concerned with theory, in a review of the responsive city, Hoffman (2016) points to the absence of and need for a theoretical framework. In response, this work explores IT implementation and the implementation concept through the research literature for the public sector in relation to digital government, eGovernment, and sensing, sensors, and the Internet of Things (IoT) in the context of smart cities. The construct of awareness and the sub-constructs of learning, openness, and engagement (for smarter and more responsive cities) are employed in this exploration in relation to the characteristics of smart cities—adaptability, complexity, innovation, and readiness—in conceptualizing more dynamic, responsive, and fluid notions and requirements for implementation in contemporary urban environments.

What follows is the development of a theoretical perspective for this work together with the conceptualization and operationalization of an ambient implementation framework; the methodology; presentation of findings; an analysis and discussion enabling the building of an explanatory model for ambient implementation including the identification of dependent and independent variables; and final remarks together with the challenges and mitigations; practical implications; and future research directions.

Perspectives on Implementation in Smarter Urban Contexts

Through a review of the research literature, perspectives are provided on smart cities, sensing, sensors, and the IoT, and the key smart city elements of adaptability, complexity, innovation, and readiness. Then, against this background, perspectives on smart cities and public sector implementations are presented, focusing on: electronic services implementation (ESI); enterprise architecture; governance infrastructures; ICT and smart global cities; IT implementation; open government and innovation; policies and programs; sustainability; and a practical example of a smart city implementation.

Smart Cities, Sensing, Sensors, and the IoT

Townsend (2013) defines smart cities as "places where information technology is combined with infrastructure, architecture, everyday objects and even our bodies, to address social, economic, and environmental problems." This definition features the intersection and interplay of urban spaces, people, and technologies that includes sensors and the Internet of the Things (IoT). In broad terms, the IoT is defined "as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (ITU 2012). The IEEE explores evolving definitions for the IoT making a distinction between small and large environments where the latter are characterized by complexity in terms of "number of things" and "things ownership/management" (IEEE 2015). Hotho et al. (2017) use the Oxford English Dictionary to define sensor as "a device which detects or measures a physical property and records, indicates, or otherwise responds to it" while extending this definition "to include technological sensors as well as human sensors."

Hotho et al. (2017) note that sensor also pertains to *sense*, defined as "a faculty by which the body perceives an external stimulus." Where "sensors and senses detect physicochemical properties of the environment," Hotho et al. (2017) point to "an extended meaning" of sensing that "relates to the psychosocial environment" as in "sensing danger" or "tension in a group of people or someone's mood" enabling "a higher level of integration and interpretation of different external and internal signals." As such, the multisensorial capabilities of people (Lévy et al. 2015) emerge as an important form of sensing as awareness. Resch (2013) claims that the people as sensors concept "defines a measurement model" where "measurements are taken by calibrated hardware sensors" and also where "humans can contribute their individual 'measurements' such as their subjective sensations, current perceptions or personal observations." Sandfort and Moulton (2015) point to the importance of behavior to "observe, take risks, and adapt" based on "what is unfolding around them." It is worth noting that Gil-Garcia et al. (2016) argue that "social infrastructure and human infrastructure are crucial axes for city development" and, as such, are important in this work for sensing and the complementing of technical sensors and IoT infrastructures.

Key elements of smart cities relevant to implementation as explored in this chapter are adaptability, complexity, innovation, and readiness.

Adaptability

Egalė et al. (2015) identify dimensions, characteristics, and criteria for smart public governance highlighting "strategic dynamics, networking, collaboration, and empowered citizenship." However, it is important to note that Cohen et al. (2016) point to an emergent "series of tensions" that are occurring "as innovators and

entrepreneurs seek to engage with local governments and citizens in an effort to improve the quality of life and promote local economic growth." Janssen and van der Voort (2016) advance the concept of adaptive governance "to deal with uncertainties and complexities" in assisting "governments in the digital age." In support of adaptability, McNutt et al. (2016) describe civic technology as "a nascent force in the relationship between governments and communities" and as an ecosystem where elements are said to include "open data, related information and communications technology (ICT) innovations and the organizational boundary-spanning practices of civic technology." Gordon and Mihailidis (2016) note that civic tech "typically refers to work within government," whereas now, this space "has grown significantly" to include many businesses, groups, and individuals.

Complexity

Sandfort and Moulton (2015) advance the view that "implementation is about making change in complex systems" and that "it is about how policy ideas become embedded in operations and everyday actions." According to Sandfort and Moulton (2015), "policy and program implementation requires continuous and intentional learning about changes." Indeed, the work of Sandfort and Moulton (2015) is informed by complex, adaptive systems where "factors are related in nonlinear ways" such that "it is difficult to anticipate the consequences of particular strategies or action." Hartemink (2016) discusses barriers to "successful implementation of smart city initiatives" emphasizing the importance of "governance as key" for such "complex projects." For Hartemink (2016), "the implementation of smart city projects is a social rather than technical thing."

Innovation

Ram et al. (2010) identify implementation as one of several processes involved in innovation. Gascó (2016) explores "what makes a city smart" by looking at the example of Barcelona as a smart city in terms of innovation and technological innovation more specifically, noting the absence of citizen participation. In the context of innovation in education, Pendleton-Jullian, in an interview with Jenkins (2016), points to the importance of the pragmatic imagination and valuing and "instrumentalizing the products of the imagination" for complex problem-solving in support of civic action. Gil-Garcia et al. (2016) conceptualize smartness in government, identifying 14 dimensions, one of which is innovation and another is openness. More recently, Gascó (2017) explores "the role of living labs as intermediaries of public open innovation" focusing on everyday contexts for experimentation in identifying the importance of "implementing an open innovation perspective." Bogers et al. (2018) describe the state of open innovation in relation to research, practice, and policy, highlighting trends such as digital transformation and the key challenge of uncertainty.

Readiness

Zygiaris (2013) identified city readiness as the fundamental and underlying layer consisting of "critical resources which will contribute to" the ability "to support the smart city vision" in order to "implement smart policies." A readiness guide was developed for smart cities in 2014 (SCC) highlighting the importance of this element for city officials. Newton et al. (2017) describe a human readiness levels (HRL) scale that "provides a framework to factor in the human dimension during technology development."

Perspectives on Smart Cities and Public Sector Implementation

Perspectives on smart city implementation are presented in this section focusing on a range of areas from electronic services implementation (ESI) to information and communication technology (ICT), to information technology (IT), and sustainability, along with a practical example of a smart city implementation.

Electronic Services Implementation (ESI)

Using institutional theory as a lens, El-Haddadeh et al. (2013) explore implementation in terms of the *complexities* of electronic services in the public sector for IT implementation and organizational transformation. Political, social, organizational, and technology forces are explored by El-Haddadeh et al. (2013) with a view to identifying and understanding key complexities. El-Haddadeh et al. (2013) include awareness among the influencing factors in the social forces category. It is worth noting that El-Haddadeh et al. (2013) find that impediments to the implementation and institutionalization process arise from the unanticipated pressures associated with the dynamic nature of technologies. Müeller and Skau (2015) identify six categories of success factors in the research literature influencing the implementation of e-government at different stages of maturity as external environment, organization, management, employees, citizens, and technology.

Enterprise Architecture

Dang and Pekkola (2017) note that enterprise architecture (EA) is employed in the public sector in support of increased efficiency and the use of information and communication technology (ICT). In order to understand more about the development, implementation, and adaptation of enterprise architecture in the public sector, Dang and Pekkola (2017) conducted a systematic review of the research literature. Findings show the need for increased research on implementation and adaptation and more particularly, for EA implementation in relation to interoperability and

integration, alignment and strategy, and pragmatic challenges (Dang and Pekkola 2017).

Governance Infrastructures

Johnston (2010) describes governance infrastructures in terms of an interactive mix of "technologies and systems, people, policies, and relationships." Going forward, Johnston (2010) advocates for "smart governance systems" as more dynamic and adaptive, in overcoming a number of issues including implementation where approaches tend to occur "through a fixed jurisdiction for a fixed period of time." Implementation is further limited by responsiveness, which, in the case of policy, is said to be incremental in nature along with the evaluation of feedback contributing to an overall slow process. In the context of technology innovations enabling e-participation in multilevel governance, Joshi and When (2017) point to the issue of project implementation confrontation, suggesting that a shift is possible through a movement away from "design–defend–implement" thinking toward "discuss–design–implement" where a space for e-participation is made in public sector governance for early stage citizen engagement as projects take form. Joshi and When (2017) point to the inclusion of "citizen discussion via social media" as a variable for e-participation explorations of people as "social sensors." In this way, people are seen to be contributing to and influencing policy discussions through "their views, sentiments, knowledge and preferences" as an added layer of open data and big data (Joshi and When 2017). Building upon the emerging research area of algorithmic governance (Danaher et al. 2017), Coletta and Kitchin (2017) explore the pulse of the city using algorhythmic governance. Bringing people more directly into the loop, Coletta and Kitchin (2017) identify the importance of exploring "the ways in which algorhythmic governance is co-created by algorithms and actors."

ICT Implementation and Smart Global Cities

Donolo and Donolo (2013) explore obstacles to implementation of the smart cities model, particularly technological infrastructures, for government authorities and their involvement of citizens. Focusing on information and communication technology (ICT) in combination with web-GIS and smart visualization, Donolo and Donolo (2013) identify physical/visible variables and virtual/invisible variables based on the representation of infrastructures and processes in urban and extra-urban zones. For Donolo and Donolo (2013), the concept of smart representation is critical to provide visualizations of urban and extra urban zone data. Anthopoulos and Fitsilis (2013) use the parameter of viability to explore technological approaches to the realization of smart city projects, finding that funding is a major determinant, among others (e.g., geographical, legal, cultural, technological, social, and environmental). Akçura and Avci (2014) claim that the implementation of smart city technologies is one of the greatest challenges for city governments. Akçura and Avci

(2014) consider macro-level variables for global city rankings and the importance of cooperation between local city and country level governments. Dependent variables are identified as: business activity, human activity, cultural experience, education, environment, stability, healthcare, and infrastructure (Akçura and Avci 2014). Multiple independent variables at the country level are identified for each of the dependent success criteria variables with ICT-related elements important for five of the eight dependent variables (Akçura and Avci 2014). Raaijen (2016) provides a framework and a checklist of vital questions for promoters or practitioners in achieving smart city success. Checklist questions are organized around the eight components of goals, challenges, governance, collaboration, societal adoption, experimenting, and solution design. Anthopoulos et al. (2016) explore smart city business models to identify how initiatives are implemented, as in the value proposition, and in turn, how value is created.

IT Implementation

Van den Bergh and Viaene (2016) explore smart city implementation in terms of six key challenges (e.g., IT alignment, organizational culture) for city administration focusing on the city of Ghent as a public sector case contributing to the study of IT-enabled transformation. One of the questions posed by Anthopoulos and Reddick (2016) addresses the theoretical capacity of eGovernment research and its evolution for smart city challenges, shedding light on "gaps, interrelationships, and reciprocities." Talari et al. (2017) provide a review of smart cities in relation to the Internet of Things, identifying major barriers to implementation as challenges (e.g., security, reliability, large scale, legal and social aspects, big data, sensor networks, demand response (DR), and heterogeneity).

Open Government and Innovation

In the context of open government, Gascó (2015) points to research on what is being implemented by governments. Gascó (2015) identifies principles (transparency, collaboration, and participation), tools, and related concepts associated with the open government concept, indicating that most initiatives focus on the opening of data for use, fostering open action. Based on the case of Government 3.0 in Korea, Nam (2015) identifies a range of challenges and concerns associated with the implementation of open government initiatives, encouraging approaches that are "more realistic, practical, and tangible" in support of gradual and increased levels of readiness. Dameri (2017) explores smart city implementation from the perspective of creating economic and public value in innovative urban systems. However, confusion and ambiguity are said to exist around the open government concept, contributing to differences in the direction and interpretation of the implementation and in turn, in the processes and impact (Giest 2017). In exploring synergies between digital government (DG) and public management (PM), Gil-Garcia et al. (2017) identify

research work that is contributing insight into factors affecting the implementation of open innovation in the public sector. Bogers et al. (2018) point to new horizons for openness and innovation policy, drawing on the Three Opens identified by the European Commission of open innovation, open science, and open to the world.

Policy and Program Implementation

Sandfort and Moulton (2015) focus on implementation in the context of public bureaucracies, extending to networks and collaboratives as well as to public–private partnerships. Implementation for Sandfort and Moulton (2015) refers to initiatives that "involve engaging others to bring about change that benefits people." According to Sandfort and Moulton (2015), implementation "requires engaging the unpredictable" in the form of "the people who shape the understanding and activities of the program at various levels" as well as "the resources of money and talent that are almost always constrained, and the political environment that is changeable." Regarding effective implementation, Sandfort and Moulton (2015) refer to the "mystery in implementation" and highlight the importance of a "social dimension" adding that effectiveness involves the cultivation of "subtle social skills that engage others in being part of the change." Sandfort and Moulton (2015) equate the success of implementation with the practical aspect of having it be "incorporated in everyday work" so as to become "part of standard operating procedures."

It is worth noting that O'Toole (2017) highlights two elements identified by Sandfort and Moulton (2015) on policy and program implementation for scholars and practitioners—the need for "adjusting to unpredictability" and the increased "tapping of creativity" in achieving effectiveness. Meijer et al. (2016) refer to the role of contextual conditions for policy implementation (e.g., smart characteristic endowments, density, wealth) in relation to governance models and public value assessment in smart city research. Focusing on big data use from a policy perspective in the public sector, Giest (2017) points to institutional barriers related to the digital component affecting implementation along with capacity-related issues.

Sustainability Implementation

Wang et al. (2012) explore the capacity to sustain sustainability itself in US cities from the perspective of capacity building in the public sector. Using a set of capacity variables (political, technical, financial, and managerial), Wang et al. (2012) contribute a capacity-building explanation for behaviors associated with sustainability implementation. Managerial capacity is found to be more significantly associated with sustainability, followed by financial and then technical capacity while citizen participation is found to have a strong association with the capacity to garner financial support. Wang et al. (2012) also explore contextual variables influencing sustainability (e.g., political, financial, environmental, and demographic/governing structures). Pointing to the critical lack of theory in support of smart city

implementation research, from an environmental sustainability perspective, Chatfield and Reddick (2016) employ a combination of resource dependence, social embeddedness, and citizen-centric e-governance theories in identifying antecedent conditions for complex smart city implementation processes, highlighting the importance of citizen engagement.

Practical Example of a Smart City Implementation

Scholl and AlAwadhi (2016) present the case of the City of Munich to demonstrate that radical ICT change in both processes and structures is possible, implementable, and achievable with success. Motivations for public sector change to smart governance included status quo dissatisfaction; perceived need for modernization; dismantling silos (departmentalism); cost pressures; efficiency gains; desire for transparency; ICT as an administrative core competency; ICT future readiness; service integration and standardization; process focus; and core competency focus (Scholl and AlAwadhi 2016). Public sector smart city implementation challenges included seven items, two of which are general resistance to change; and finding and implementing a transparent and effective decision-making process (Scholl and AlAwadhi 2016).

Summary

For the public sector, implementation challenges emerge in the research literature in relation to digital or electronic approaches pertaining to policy, governance, and government processes including openness, innovation, and infrastructures. An overview is provided in Table 1 of implementation perspectives for smart cities, sensing, sensors, and the IoT, highlighting the importance of an awareness of adaptability, complexity, innovation, and readiness. Learning, openness, and engagement are featured here as critical to the development and use of infrastructures for sensing, sensors, and the IoT.

Learning emerges as important for adaptability, complexity, innovation, and readiness in terms of governance, change, experimentation, and resources. Openness emerges as important for adaptability, complexity, innovation, and readiness in terms of collaboration, governance, smartness, and the human element of people. Engagement emerges as important for adaptability, complexity, innovation, and

Table 1 Overview of implementation perspectives on smart cities, sensing, sensors, and the IoT

Awareness	Adaptability	Complexity	Innovation	Readiness
Learning	Governance	Change	Experimentation	Resources
Openness	Collaboration	Governance	Smartness	People
Engagement	Citizens	Social	Processes	Policies

Table 2 Overview of smarter implementation conditions, determinants, variables, and factors

Implementation	Conditions	Determinants	Variables	Factors
eGovernment				Success
eServices (ESI)				Awareness
EA (Architecture)				Integration
Governance			Social sensors	Smartness
ICT		Funding	City rankings	
ICT Infrastructure			In/Visible	
IT				Challenges
Open Government				Varied
Policy	Contextual			Social
Sustainability	Antecedent		Capacity	
Munich Example				Challenges

readiness in terms of people, social, processes, and policies. Table 2 provides an overview of conditions, determinants, variables, and factors influencing approaches to smarter implementation that emerged from a review of the literature for perspectives on smart cities and public sector implementation.

For example, success factors are identified for eGovernment implementation; awareness factors for electronic services implementation (ESI); integration and other factors for enterprise architecture implementation; citizen discussion via social media as a variable for explorations of people as social sensors for governance implementation; funding is identified as a determinant for ICT implementation and macro-level variables for city rankings are identified; physical/visible variables and virtual/invisible variables are identified for the representation of infrastructures and processes; IT implementation barriers are identified as challenges; varied factors emerge as affecting open government and innovation implementation; contextual conditions and social factors are identified for policy implementation; antecedent conditions and capacity variables (e.g., political, technical, financial, and managerial) emerge for sustainability implementation; and Munich is described as an example of a smart city implementation along with the identification of motivations and challenges.

In addition to conditions, determinants, variables, and factors influencing the various types of implementation, the parameter of viability is identified in relation to ICT and forces such as political, social, organizational, and technology are identified for ESI. Theories used by researchers include institutional theory in the study of complexities in ESI (El-Haddadeh et al. 2013) and a combination of resource dependence, social embeddedness, and citizen-centric e-governance theories (Chatfield and Reddick 2016) are used for smart city implementation.

Conceptualizing an Adaptive Implementation Framework

In view of the dynamic nature of evolving urban environments, this work conceptualizes a more adaptive implementation framework to accommodate sensing, sensors, and the IoT in the public sector in support of smarter cities. As such, the ambient implementation concept is advanced in this work focusing on practical approaches and solutions for the everyday world where in-the-moment response(s) are required and enabled by more aware people and aware technologies in the form of sensing, sensors, and the IoT, in the context of smart cities. Theoretically, this work is situated at the intersection of the physical and services layers of urban infrastructures on the one hand and the emerging digital/data layer(s) (Finger 2016) on the other, in coming to new understandings of more dynamic, adaptive, and responsive implementation challenges as opportunities for the public sector in smart cities. As illustrated in Fig. 1, through the interactive dynamic of *people—technologies—cities*, public sector approaches to the emerging mechanisms of sensing, sensors, and the IoT are explored in relation to adaptability, complexity, innovation, and readiness as key elements of smart cities, posing particular implementation challenges as opportunities.

This work is operationalized using the construct of *awareness* in relation to aware people in combination with aware technologies. The sub-constructs of *learning—openness—engagement* are also employed in contributing to emergent and more enriched understandings of the notion of ambient implementation as continuous and evolving, extending to public and more people-centered spaces.

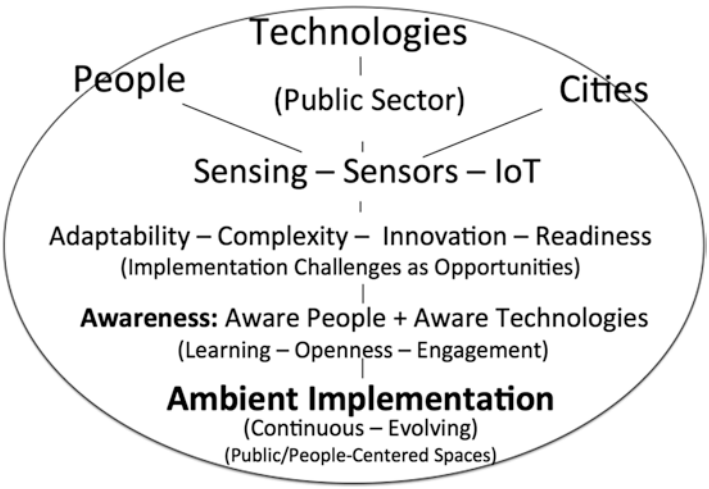


Fig. 1 Ambient implementation framework for public sector sensing, sensors, and the IoT

Methodology

The research design for this work incorporates a single case study approach with multiple methods of data collection, including interview and survey. In support of this approach, Paré and Elam (1997) point to the importance of case study research when investigating the dynamic nature of IT phenomena and Yin (2018) points to the value of this approach for investigating a contemporary phenomenon in context. The research question and proposition; process; data sources; analysis techniques; and conceptualizing of an adaptive implementation framework for this study are described below.

With the purpose to explore and shed light on new, more dynamic and adaptive understandings of implementation in contemporary urban contexts, enabled and influenced by aware people and aware technologies (sensing, sensors, and the IoT) in the public sector in the context of smart cities, this work uses the construct of awareness to investigate the following research question:

Q1: In twenty-first century urban environments, why do sensing, sensors, and the IoT present important implementation challenges for the public sector related to awareness?

The research question is reformulated here as a proposition for exploration in this chapter, as follows:

P1: In twenty-first century smart urban environments, awareness in the form of more aware people in combination with aware technologies forms the basis for more effective and dynamic implementation, as in ambient implementation, of sensing, sensors, and the IoT in the public sector, contributing to greater challenges as opportunities for *adaptability*, *readiness*, and *innovativeness* in response to increasing *complexities*.

A website was used to describe the study, enable sign-up, the gathering of basic demographic data, and self-identification in one or more categories (e.g., educator, student, community member, city official, business, and other). Participants were invited to complete an online survey and to engage in an in-depth discussion of their experience of smartness in their city or community through an interview (online or in person). Over a 2- to 3-year period (2015–2018) the study attracted interest from individuals, mostly in Canada but also extending to other countries and cities such as Israel (e.g., Tel Aviv).

Online posting of the study invitation was made to webspaces that would attract researchers, practitioners, and anyone interested in smart cities. Sampling procedures consisted of purposive sampling, more specifically, heterogeneity sampling, to accommodate a broad spectrum of perspectives (Trochim 2006). Discussions were conducted with diverse individuals, in the context of smart cities, about technology-infused city spaces focusing on elements of smartness related to sensing, sensors, and the Internet of Things (IoT).

Sources of Evidence and Data Analysis

An interview protocol and a survey instrument were developed and pre-tested prior to use in the study. Three of the 20 questions appearing in the survey instrument are as follows: (1) What does smartness look like in your city (smartphones, smart meters, urban displays/screens/sensors, drones, etc.)? (2) In your opinion, what contributes to the making of a smart city? (3) How would you say social media and other aware technologies are affecting your experience of the city? Three of the 12 questions appearing in the interview protocol are as follows: (1) What enables you to feel the pulse of the city? In other words, how do you sense the city? (2) What do you think about smartness in cities? (3) How do you think the increasing presence of information and awareness, as in ambient, is affecting your experience of being in the city?

In addition to questions about smart cities, the interview protocol and the survey instrument contained three questions pertaining to sensing, based on a sample version of Anderson's body intelligence scale (BIS) (2006). The BIS, now referred to as the body insight scale (http://rosemarieanderson.com/e-brary/), was slightly modified in this work for use in contemporary urban environments. Additionally, the scale was revised from a 5-point to a 7-point scale to allow for greater flexibility in response. Rationale for use of Anderson's BIS is based on the need for a scale designed for use with people, to detect human awareness and sensing by humans. Other scales tend to focus on human sensing using computing technologies for the detection of such things as presence, count, location, track, and identity (Teixiera et al. 2010).

In parallel with this study, data were systematically gathered from diverse voices (e.g., city officials, business, educators, students, community members, and IT staff) in meetings about smart cities, organized with individuals and groups (e.g., Toronto, Vancouver, Victoria). Discussions conducted in these meetings were also guided by the case study interview protocol.

As qualitative data were gathered from interviews, group and individual discussions, and open-ended survey questions, analysis began immediately and iteratively. Content analysis, pattern matching, and explanation building were employed in the analysis of data. During content analysis, deductive analysis was conducted based on terminology from the research literature and inductive analysis was conducted based on emergent terms and concepts from the collected data. The three data streams (interviews, discussions, and open-ended survey responses) enabled simultaneous analysis, comparison, and triangulation. Descriptive statistics were used to analyze sensing data gathered from questions using the BIS (body insight scale) and survey questions.

Overall, an analysis was conducted for $n = 61$ consisting of 39% females and 61% males for people ranging in age from 20 to 70 years.

Findings

Findings are presented in response to the research question, based on the proposition explored in terms of the construct of awareness and the sub-constructs of learning, openness, and engagement and what people said.

An interweaving of the construct, sub-constructs, and smart city characteristics as interactive elements is reflective of the emergent findings in terms of challenges as opportunities for ambient implementation as depicted in Fig. 2.

The construct of awareness; sub-constructs of learning, openness, and engagement; and discussion threads will be aligned as interactive elements with adaptability, complexity, innovation, and readiness in coming to new understandings of the challenges as opportunities and potentials for the public sector in relation to more dynamic implementations of aware technologies (e.g., sensing, sensor, and the IoT) as ambient.

Awareness and Adaptability

In response to whether *Awareness in the form of more aware people in combination with aware technologies forms the basis for more effective and dynamic implementation, as in ambient implementation, of sensing, sensors, and the IoT in the public sector, contributing to greater challenges as opportunities for adaptability, readiness, and innovativeness in response to increasing complexities*, individuals indicated in survey responses that to become smarter, cities need to "make engagement smarter (e.g., break down the silos and collaborate more" as well as "make participation smarter (e.g., remove the red tape and bureaucracy)." Tourism and the "layers of what's happening" in the city were identified by a community member in Greater Victoria in terms of a digital strategy for art, culture, music, and the like. City IT staff indicated that "we furnish some of the elements of engagement." The example of an eTownHall meeting was mentioned "because we've brought technology" to the space enabling "bringing questions in and sharing answers through Twitter" and other social media enabling "another level of engagement that our Citizen Engagement Department was very interested in because it gave them a dataset that was above and beyond" the usual, contributing to "documented engagement." Budgeting was described as "another area where there is a tool for the public to

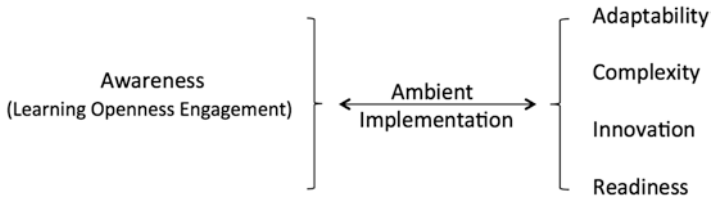


Fig. 2 The interweaving of interactive elements for ambient implementation

engage and play" enabling people to get "a sense of where the cost pressure points" are "around decision making" by turning the dial up or down on various services. A student identified "data visualizations rather than just urban displays" as important for "getting people involved." Referring to "city dashboards" the student suggested that "you can take these bits of data and make beautiful artistic visualizations" and "this is how to get people on board." A community member in St. John's suggested the need for "not too dense information on what's happening at a particular point so that you can access this type of information and know what's going on in real time almost" using the example of cellphone parking lots at airports and the smartness aspect that "decreases congestion." An educator pointed to the need "to focus on technology" in terms of "what it is for" in that it "enables people to capture evidence of their activities, actual evidence of the contribution" in order to "answer some questions" and "ideate about problems in the city." Highlighting the opportunity for city officials "to listen and understand what people want in the form of evidence" this individual made reference to the importance of the "will and ability and the resolve to implement some of those things." A community member in Toronto noted that "creating a more engaged citizenry" involving the use of "technology and social media working together" could be realized based on urban issues such as a "development proposal" since it "affects everybody because their environment is being changed." An urban public engagement consultant spoke of "digital engagement" and "the apps and engagement tools" such as PlaceSpeak as a mechanism "to encourage people to do some observations of space and people." Little free libraries, as pocket spaces with things in the form of books were described to illustrate "there is human interaction, the technology and the space" as "parts of the same puzzle." Technology was also considered as "a way to animate a space" as an engagement mechanism.

Awareness and Complexities

Considering whether *Awareness in the form of more aware people in combination with aware technologies forms the basis for more effective and dynamic implementation, as in ambient implementation, of sensing, sensors, and the IoT in the public sector, contributing to greater challenges as opportunities for adaptability, readiness, and innovativeness in response to increasing complexities*, people responded with an immediacy about their ability for sensing in the urban environment. For example, Table 3 shows sensing responses using the body insight scale (BIS) for three questions, pertaining to awareness in the city, as follows:

Table 3 Body Insight Scale (BIS) responses for city-based feelings of safety, comfort, and anger

Awareness	1	2	3	4	5	6	7
Energy body: safety		33%					67%
Comfort body			67%				33%
Inner body: tightens/angry				33%	33%	33%	

1. Would you agree that your body lets you know when your environment is safe?
2. Would you agree that you feel comfortable in your city most of the time?
3. Would you agree that you can feel your body tighten up when you are angry?

People tended to respond at the upper end of the seven-point scale (disagree at the lower end and agree at the upper end) in response to the question about feeling safe (67%), although a 33% response rate emerges near the lower end at position 2. The question about comfort revealed additional complexity with only 33% of responses at the upper end and 67% toward the lower end in position 3. Regarding body tightness and the emotion of anger, still more complexity emerged with 33% responding in the neutral zone and 33% toward the upper end at positions 5 and 6.

Probing further using qualitative data from interviews to better understand this quantitative data, people indicated how their scale rating would change if they were in a different or larger city. Complexities emerged in terms of comfort in the city, associated with understandings of what contributes to comfort in terms of urban planning, revealing that the design and placement of urban elements such as benches, affected scale ratings. An individual from a relatively small (population under 400,000) but densely populated city found it difficult to imagine experiencing body tension associated with anger but then recalled tension arising "if you can't find a parking place" while identifying the problem of "the traffic" described as "the least smart thing" in the city.

In an open-ended survey question, when asked, "How do you sense the city?" individuals referred to the people component, as in, "human activity in every corner" and "the gatherings created from various festivals" and "the multi layers of senses." In assessing whether "city-focused social media and aware technologies" give rise to the potential for "attuning to urban spaces," survey respondents provided ratings at the upper end of the scale (7) with 67% indicating absolutely and 33% at position 6 on the scale. In coming to an understanding of this response, in the qualitative data, referring to the iPhone, a community member commented that "there are a lot of advantages to having that to enhance the urban experience" in terms of being "able to get from point a to b faster or maybe find something out about the area." A community leader acknowledged the value of the Victoria ParkingApp that enables people to pay for parking on the go. As if to provide an example of Pendleton-Jullian's notion of the instrumentalizing of the products of the imagination, the community leader suggested the idea of extending the ParkingApp to "help me find parking." A community member in St. John's wondered whether "one's senses are more technologically aware in large cities than small." An educator noted the "videoing and sharing of very traditional things constantly in social media" and the notion of "concurrent awareness" enabling "seamless behavior" also evident in the "seamless interrelationship of" the "local and global."

An IT developer providing services to municipal governments and postsecondary institutions in Greater Victoria and Vancouver observed that there are "a lot of moving pieces to make a smart city." Referring to the complexity of smart cities, this individual noted that "implementation is going to be the biggest challenge" because "everything about it would have to be dynamic, down to managing the dif-

ferent departments." An individual in the technology business described the potential for city IT to build a public network in support of city infrastructure and services—to run traffic lights, municipal buildings, and water and sewage, noting that "it's all getting smart" and with excess bandwidth, the question was raised, "could that bandwidth be used to drive economic value to the city?" City IT noted that "almost any technology now has the ability to be more than just a single service" highlighting "more intelligent lighting" as in "lighting whenever people need it" indicating that "an intelligent fabric to communicate enables so much more." For example, reference was made to the potential for "putting sensors in garbage cans so they tell you when they're full" which "reduces the number of visits or increases the number" resulting in a push for "starting to instrument more and more of those elements." Indeed, the IoT was viewed as "more about the instrumentation of things, with everything connected and communicated."

Awareness and Innovation

In response to whether *awareness in the form of more aware people in combination with aware technologies forms the basis for more effective and dynamic implementation, as in ambient implementation, of sensing, sensors, and the IoT in the public sector, contributing to greater challenges as opportunities for adaptability, readiness, and innovativeness in response to increasing complexities*, survey respondents associated openness with smart cities as indicated by 33% ratings at the upper end of the scale (7), 33% ratings at 6 on the scale and 33% at the neutral position of 4 on the scale. City IT staff in Greater Victoria commented that "fundamentally there is a desire to be very, very open with the available data" as public data. It was noted that "the other element we're trying to share is even just the processes of City Hall" using the example of permit applications. City IT staff added that open, diverse datasets enable "data analysis that you've not thought of" supporting the potential for "serendipitous or accidental usage" or "unintended usage" and unforeseen value. Providing an example from business, such usage revealed "a win that wasn't even in our mindset" where staff "were using it as a predictive piece to inform their daily operations." The "challenge of asset management" was identified by City IT adding that "we are interested in putting physical infrastructure in place" and "how we interpret using it is still open," identifying challenges that include jurisdictional ones in terms of "a hard stop at municipal boundaries." Speaking of wicked challenges, a student identified "control" as in "who owns the data, how is it housed, and the infrastructure by which it is shared." The student pointed to the potential for the data to be "open and shared in some way that would still provide some kind of smart delivery so you could actually make use of the data" as in "learning data, information data about, things, events, places" and so on. The student noted that "the more that technical infrastructure can be made to constantly reciprocate the data flows that are happening between people, formal and informal, the better" in support of the "goal of smart cities."

Awareness and Readiness

In response to whether *awareness in the form of more aware people in combination with aware technologies forms the basis for more effective and dynamic implementation, as in ambient implementation, of sensing, sensors, and the IoT in the public sector, contributing to greater challenges as opportunities for adaptability, readiness, and innovativeness in response to increasing complexities*, individuals indicated in survey responses that "people generally are not aware of smart cities." City IT staff highlighted the phenomena of "accidental data collection" and data that "I don't think anybody saw a need for." Additionally, it was noted that "we're starting to look at the tools to help us mine the data that we already have an interest in" and "beyond that, we're very much immature in that overall data sense." For example, it was indicated that looking at data "between two different datasets, we're just starting to look at the tools that would give us the visualization of that" in lieu of any "practical application." City IT staff commented on "that hurdle of just really starting to educate" about "what could be done" and "educating ourselves." The additional hurdle was noted that "we haven't had any kind of funding to do these things."

Learning was envisioned by a community member based on the use of technologies "to experience the city in a different way" in terms of "the environment or the history" to "create different games or opportunities for people" and to "make cities more friendly for our kids." This individual suggested "there is a whole other layer that could be added in order to make the city more usable for everybody." As if in support of such a layer, City IT staff described digital infrastructure planning, noting that "we've started that process so engineering is putting in communication and ducting it for every cross-section" so that in terms of readiness "there is a little bit of forward thinking" and "so we're lowering the overall cost of doing it in the future." And cost was highlighted by city IT staff regarding "the equipment" for "smart traffic signals" although this infrastructure "would significantly improve the congestion." Described as being "in its infancy" the use of drone technology to capture aerial photos of the city was identified, extending also to the fire department for "search and rescue and safety operations." The importance of relationships were identified in terms of the responsibility for the official city plan by "the Planning Department" where "IT is brought in to implement" as is Engineering. A community member in St. John's observed that "we're not smart on how we use the technology" citing "improved communications about the transportation system" and "anywhere Internet" as being key priorities that would be "particularly useful." A city councilor in Greater Victoria spoke of technology "as a tool that will allow people to connect to each other and to their surroundings" adding that "vibrancy is created by people and connections between people and the way that comes to life" is by "creating activity." A student discussed "geofenced location based content" that is "connected in relation to community interactions" with the idea that "learning becomes a subsumed subtext of what you are doing every day, all the time" in support of continuous forms of learning that could be "formal, informal, fun, serious."

Discussion: Explanatory Model for Ambient Implementation

A discussion of findings is presented contributing to the building of an explanatory model for ambient implementation. An analysis of findings in this chapter enables the building of an awareness-based explanatory model for ambient implementation in relation to sensing, sensors, and the IoT in smart cities. Awareness and adaptability, awareness and complexity, awareness and innovation, and awareness and readiness are identified as dependent variables (DV) that can be observed and measured in relation to the independent variables (IV) identified for each in this work, as presented in Fig. 3. Independent variables for sensing, sensors, and the IoT in the public sector emerging from this work for each of the dependent variables include, but are not limited to, the following:

Awareness and Adaptability (DV)

Independent Variables

Digital strategy for urban events; documented engagement; artistic data visualization; technology to animate spaces. Urban infrastructural improvements involving the incorporation and enhancement of the human element (meaningful engagement of people) and the digital and data layers enable more adaptive, innovative, and complex supports and services for the use of sensing, sensors, and the IoT.

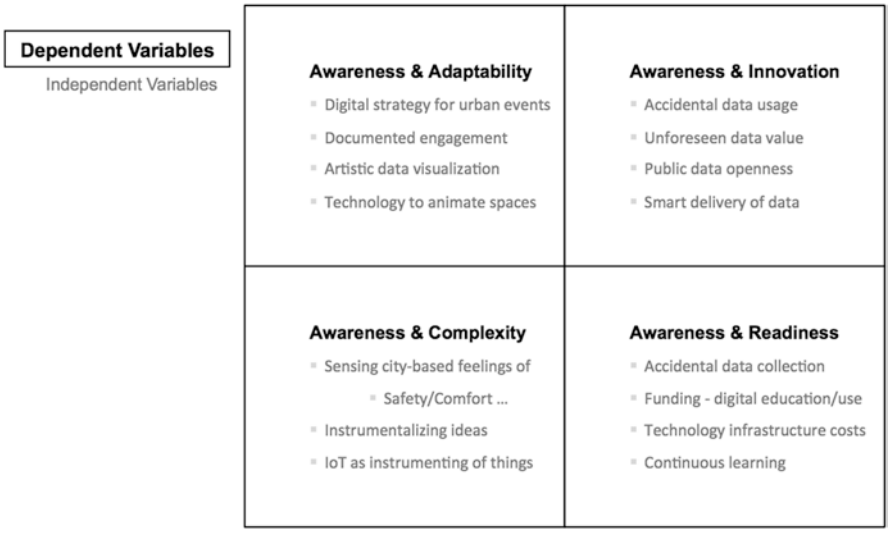


Fig. 3 Awareness-based ambient implementation explanatory model for smart cities

Awareness and Complexity (DV)

Independent Variables

Sensing city-based feelings of comfort, safety, and other affective/emotive responses; instrumentalizing ideas as products of the imagination; the IoT as the instrumenting of things. Human capabilities for acute sensing in urban areas, when combined with other analytic tools and aware technologies, from smartphones to social media to urban displays with embedded sensors were understood to augment and enhance the experience of the city. The readiness of people to attune to their city and provide assessment data on a sensory level for safety, comfort, and tension-related anger was shown in Table 3 in this early-stage, exploratory application of the BIS (body insight scale) to provide insight into the complexities of contemporary urban environments.

Awareness and Innovation (DV)

Independent Variables

Accidental data usage; unforeseen data value; public data openness; smart delivery of data. Seeking to respond to contemporary urban needs, city IT staff highlighted the ongoing mix and balancing of developing processes including adaptability, innovation, and readiness, in the face of ever increasing complexities associated with funding, infrastructure development and maintenance, the evolving of more collaborative practices, jurisdictional issues, and so on.

Awareness and Readiness (DV)

Independent Variables

Accidental data collection, funding for digital education and data use; technology infrastructure development costs; continuous learning. As city administration, business, community members, educators, students, and people in the city become more engaged with each other, the potential emerges for more aware people interacting with aware technologies in more meaningful ways, creating greater readiness for the implementation of smarter cities, and for new understandings of implementation as ambient.

Final Remarks

This chapter explores emerging understandings of implementation in relation to sensing, sensors, and the Internet of Things (IoT) in the public sector in the context of the smart city characteristics of adaptability, complexity, innovation, and readiness. The construct of awareness and the sub-constructs of learning, openness, and engagement provide a lens for this exploration. The main contributions of this work include (a) the use of an awareness perspective to explore implementation challenges as opportunities for aware technologies such as sensing, sensors, and the IoT; (b) development and operationalization of an ambient implementation framework for public sector sensing, sensors, and the IoT as more adaptive, dynamic, and responsive; (c) exploration of human sensory capabilities through the early-stage adaptation of the BIS (body insight scale) for use in the context of contemporary urban environments to complement and extend existing and emerging uses of sensing, sensors, and the IoT; and (d) building of an awareness-based explanatory model for ambient implementation with the identification of independent and dependent variables for public sector sensing, sensors, and the IoT.

A key challenge of this work is the small sample size and this was mitigated by in-depth interviews from diverse individuals across multiple cities in several countries. Challenges associated with elements such as geographic location and city size are mitigated by the potential to extend this study to other cities and mega-regions exceeding ten million people in size. Understanding the nature of embedded and often invisible infrastructures, whether physical (e.g., in the form of underground wires and pipes and the like) or digital (e.g., in the form of sensors and the IoT) or human (e.g., in the form of sensing and social interactions), presented challenges that were mitigated by in-depth discussion, everyday examples, and the adaptation and exploratory use of a scale (BIS) for "assessing subtle human qualities" (Anderson 2006) in contemporary urban environments.

The small sample size achieved for this study does not support the development of statistical significance or generalizability. However, the study enables analytic generalizations of case study findings to theory (Yin 2018). This type of empirical to theoretical generalizability (Lee and Baskerville 2003) may hold important implications for other explorations of awareness-based sensing, sensors, and the IoT and the dependent and independent variables identified in Fig. 3 in terms of more dynamic, adaptive, and responsive understandings of implementation as ambient in smart city contexts. Going forward, this work has practical implications for implementations of sensing, sensors, and the IoT in public sector practice in the context of smart cities and learning cities. For example, this work evolves implementation challenges for practitioners in the public sector by presenting several practical opportunities, as follows:

Smarter infrastructures—Expanding understandings of urban infrastructure beyond roads and pipes and wires to include human infrastructures and digital and data infrastructures that are aware, interactive, and adaptive. A practical example of "instrumentalizing the products of the imagination" (Jenkins 2016) is the mean-

ingful engagement of people in the developing and extending of a civic application for parking, in urban planning discussions, and in input into community discussions contributing to problem-solving, solution generation, and decision-making.

Smarter implementation—Fostering the development of urban initiatives involving meaningful engagement opportunities in combination with the use of aware technologies such as art in public places incorporating sensing, sensors, and the IoT to animate urban spaces.

Smarter data usage—Providing increased openness, funding, innovative spaces, and learning opportunities for the creative and meaningful use of new data streams drawing on sensing, sensors, and the IoT. Leveraging data for smarter usage serves to contribute to new forms of public sector value while supporting the exploration, testing, and validating of the dependent and independent variables identified in Fig. 3 in this work.

Going forward, this work has implications for implementations of sensing, sensors, and the IoT in public sector research in the context of smart cities and learning cities. For example, this work evolves implementation theory for researchers in the public sector by identifying several directions for future research, as follows:

Aware people and aware technologies—Explore the leveraging of human sensory capabilities (sensing) as aware people to complement and extend the technical capabilities of aware technologies, including sensors and the IoT, in urban spaces. Recognizing the potentials of human insights (HI) may serve to complement and extend the potential of AI (artificial intelligence).

BIS (body insight scale)—Further exploration, extending, adapting, and validating of the BIS for use in contributing to the ambient implementation explanatory model for sensing, sensors, and the IoT in relation to aware people and aware technologies for smarter urban environments.

Everyday, in-the-moment focus—Further development, exploration, and theorizing of the ambient implementation concept focusing on everyday, in-the-moment interactions, initiatives, and issues as opportunities for investigation of the dependent and independent variables identified in Fig. 3 in this work.

A key take away from this work is the potential and value of an awareness-based explanatory model for ambient implementation to provide novel forms of smart city metrics for the public sector in support of the dynamic, adaptive, and responsive nature of sensing, sensors, and the IoT technologies while improving human engagement and solution-making in the face of complex urban challenges. This work will be of interest to a broad audience including educators, students, city officials, businesses, community leaders, urban professionals, and anyone concerned with smarter approaches to the implementation of sensing, sensors, and the IoT in the public sector in contemporary urban environments.

References

Akçura, M. T., & Avci, S. B. (2014). How to make global cities: Information communication technologies and macro-level variables. *Technological Forecasting & Social Change, 89*(C), 68–79.

Anderson, R. (2006). Body intelligence scale: Defining and measuring the intelligence of the body. *The Humanist Psychologist, 34*(4), 357–367.

Anthopoulos, L., & Fitsilis, P. (2013). Using classification and roadmapping techniques for smart city viability's realization. *Electronic Journal of e-Government, 11*(1), 325–336.

Anthopoulos, L. G., & Reddick, C. G. (2016). Understanding electronic government research and smart city: A framework and empirical evidence. *Information Polity, 21*(1), 99–117.

Anthopoulos, L., Fitsilis, P., & Ziozias, C. (2016). What is the source of smart city value? A business model analysis. *International Journal of Electronic Government Research, 12*(2), 56–76.

Bogers, M., Chesbrough, H., & Moedas, C. (2018). Open innovation: Research, practices, and policies. *California Management Review, 60*(2), 5–16.

Charoubi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., & Scholl, H. J. (2012). Understanding smart cities: An integrative framework. In *Proc of the 45th HICSS* (pp. 2289–2297). Piscataway, NJ: IEEE.

Chatfield, A. K., & Reddick, C. G. (2016). Smart city implementation through shared vision of social innovation for environmental sustainability: A case study. *Social Sciences Computer Review, 34*(6), 757–773.

Cohen, B., Almirall, E., & Chesbrough, H. (2016). The city as lab: Open innovation meets the collaborative economy. *California Management Review, 59*(1), 5–13.

Coletta, C., & Kitchin, R. (2017). Algorhythmic governance: Regulating the 'heartbeat' of a city using the Internet of Things. *Big Data & Society, 4*, 1–16.

Dameri, R. P. (2017). *Smart city implementation: Creating economic and public value in innovative urban systems. Progress in IS series*. New York, NY: Springer.

Danaher, J., Hogan, M. J., Noone, C., Kennedy, R., Behan, A., De Paor, A., Felzmann, H., Haklay, M., Khoo, S. M., Morison, J., Murphy, M. H., O'Brolchain, N., Schafer, B., & Shankar, K. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big Data & Society, 4*, 1–21.

Dang, D., & Pekkola, S. (2017). Systematic literature review on enterprise architecture in the public sector. *The Electronic Journal of e-Government, 5*(2), 132–154.

Donolo, R. M., & Donolo, M. (2013). How to achieve smart cities through smart communication and representation of urban data. In *29th Urban Data Management Symposium, International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, London, UK* (Vol. XL-4/W1, pp. 83–86). Göttingen: Copernicus Publications.

Egalė, G., Jurgita, Š., & Jolanta, S. (2015). *Smart public governance: Dimensions, characteristics, criteria*. Paper presented at the International Research Society for Public Management (IRSPM) Conference, pp. 1–13.

El-Haddadeh, R., Weerakkody, V., & Al-Shafi, S. (2013). The complexities of electronic services implementation and institutionalization in the public sector. *Information & Management, 50*(4), 135–143.

Finger, M. (2016). *Smart cities – Management of smart urban infrastructures. (Massive Open Online Course)*. Lausanne: École Polytechnique Fédérale de Lausanne.

Gascó, M. (2015). Special issue on open government: An introduction. *Social Science Computer Review, 33*(5), 535–539.

Gascó, M. (2016). What makes a city smart? Lessons from Barcelona. In *Proceedings of the 49th HICSS* (pp. 2983–2989). Piscataway, NJ: IEEE.

Gascó, M. (2017). Living labs: Implementing open innovation in the public sector. *Government Information Quarterly, 34*(1), 90–98.

Giest, S. (2017). Big data for policymaking: Fad or fasttrack? *Policy Sciences, 50*(3), 367–382.

Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2016). Conceptualizing smartness in government: An integrative and multi-dimensional view. *Government Information Quarterly, 33*(3), 524–534.

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2017). Digital government and public management research: Finding the crossroads. *Public Management Review, 20*(5), 633–646.

Gordon, E., & Mihailidis, P. (2016). *Civic media: Technology, design, practice*. Cambridge, MA: MIT.

Hartemink, N. A. (2016). *Governance processes in smart city initiatives: Exploring the implementation of two Dutch smart city projects: TRANSFORM Amsterdam and TRIANGULUM Eindhoven*. Unpublished doctoral dissertation. TU Delft. Retrieved May 9, 2017, from TU Delft Repository link.

Hoffman, M. C. (2016). The responsive city: Big data versus big government. *Public Administration Review, 76*, 684–686.

Hotho, A., Stumme, G., & Theunis, J. (2017). New ICT-mediated sensing opportunities. In V. Loreto, M. Haklay, A. Hotho, V. D. P. Servedio, G. Stumme, J. Theunis, & F. Tria (Eds.), *Participatory sensing, opinions and collective awareness*. Cham: Springer.

IEEE. (2015). *Towards a definition of the Internet of Things (IoT)*, Revision 1. IEEE Internet Initiative. Retrieved June 18, 2017, from http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

ITU. (2012). *Overview of the internet of things, Y.2060*. IoT-GSI. International Telecommunications Union. Retrieved June 18, 2017, from https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

Janssen, M., & van der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly, 33*(1), 1–5.

Jenkins, H. (2016). *Mapping the pragmatic imagination: An interview with Ann M. Pendleton-Jullian*. (Part 3). Blog. Retrieved December 16, 2016, from http://henryjenkins.org/2016/11/mapping-the-pragmatic-imagination-an-interview-with-ann-m-pendleton-jullian-part-3.html.

Johnston, E. (2010). Governance infrastructures in 2020: Part I: The good, the bad, and the ugly. *Public Administration Review, 70*, S122–S128.

Joshi, S., & When, U. (2017). From assumptions to artifacts: Unfolding e-participation within multi-level governance. *The Electronic Journal of e-Government, 15*(2), 116–129.

Konomi, S., & Roussos, G. (2017). *Enriching urban spaces with ambient computing, the Internet of Things, and smart city design*. Hershey, PA: IGI Global.

Lee, A., & Baskerville, R. (2003). Generalizing generalizability in information systems research. *Information Systems Research, 14*(3), 221–243.

Lévy, J., Beaude, B., Poncet, P., Noizet, H., Laurent-Lucchetti, B., Bahrani, F., Maitre, O., Bataille, T., Tiphine, L., Yan, L., Tursic, M., & Rommany, T. (2015). *EPFLx: SpaceX exploring humans' space: An introduction to geographicity. Massive Open Online Course (MOOC), edX, Fall*. Lausanne: EPFL.

McNutt, J. G., Justice, J. B., Melitski, J. M., Ahn, M. J., Siddiqui, S. R., Carter, D. T., & Kline, A. D. (2016). The diffusion of civic technology and open government in the United States. *Information Polity, 21*(2), 153–170.

Meijer, A. J., Gil-Garcia, J. R., & Rodriguez Bolivar, M. P. (2016). Smart city research: Contextual conditions, governance models, and public value assessment. *Social Science Computer Review, 34*(6), 647–656.

Müeller, S. D., & Skau, S. A. (2015). Success factors influencing implementation of e-government at different stages of maturity: A literature review. *International Journal of Electronic Governance, 7*(2), 136–170.

Nam, T. (2015). Challenges and concerns of open government: A case of government 3.0 in Korea. *Social Science Computer Review, 33*(5), 556–570.

Nam, T., & Pardo, T. A. (2011). Smart city as urban innovation: Focusing on management, policy, and context. In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV2011)* (pp. 185–194). New York, NY: Association for Computing Machinery.

Newton, V., Greenberg, A., & See, J. (2017). Project management implications and implementation roadmap of human readiness levels. In F. F.-H. Nah & C.-H. Tan (Eds.), *HCIBGO, Part I, LNCS 10293* (pp. 99–111).

O'Toole, L. J. (2017). Implementation for the real world (book review). *Journal of Public Administration Research and Theory, 27*(2), 376–379.
Paré, G., & Elam, J. J. (1997). Using case study research to build theories of IT implementation. In A. S. Lee, J. Liebenau, & J. I. deGross (Eds.), *Information systems and qualitative research* (pp. 542–568). London: Chapman and Hall.
Raaijen, T. (2016). Depicting the smarter cities of the future: A systematic literature review and field study. In *25th Twente Student Conference. Enschede, The Netherlands*. Piscataway, NJ: IEEE.
Ram, J., Cui, B., & Wu, M. -L. (2010). The conceptual dimensions of innovation: A literature review. *Proceedings of the International Conference on Business & Information*. Retrieved May 9, 2017, from http://hdl.handle.net/2440/65701.
Resch, B. (2013). People as sensors and collective sensing – Contextual observations complementing geo-sensor network measurements. In J. M. Krisp (Ed.), *Progress in location-based services* (pp. 391–406). New York, NY: Springer.
Sandfort, J., & Moulton, S. (2015). *Effective implementation in practice: Integrating public policy and management*. San Francisco, CA: Jossey-Bass. 388 pp.
SCC. (2014). *Smart cities readiness guide, v 2.0.* Reston, VA: Smart Cities Council. Retrieved May 9, 2017, from http://readinessguide.smartcitiescouncil.com.
Schmitt, G. (2017). *Responsive cities*. Zurich: Future Cities Laboratory, ETH. Retrieved March 7, 2018, from http://www.fcl.ethz.ch/research/responsive-cities.html.
Scholl, H. J. (2016). Special issue on "smartness in governance, government, urban environments, and the Internet of Things": An editorial introduction. *Information Polity, 21*(1), 1–3.
Scholl, H. J., & AlAwadhi, S. (2016). Creating smart governance: The key to radical ICT overhaul at the City of Munich. *Information Polity, 21*(1), 21–42.
Talari, S., Shafie-khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. P. S. (2017). A review of smart cities based on the Internet of Things concept. *Energies, 10*(4), 1–23. https://doi.org/10.3390/en10040421.
Teixiera, T., Dublon, G., & Savvides, A. (2010). A survey of human-sensing: Methods for detecting presence, count, location, track, and identity. *ENALAB Technical Report, 1*(1), 1.
Townsend, A. M. (2013). *Smart cities: Big data, civic hackers and the quest for a new utopia*. New York, NY: WW Norton.
Trochim, W. M. K. (2006). *Research methods knowledge base*. Retrieved December 15, 2011, from http://www.socialresearchmethods.net/kb.
Van den Bergh, J., & Viaene, S. (2016). Unveiling smart city implementation challenges: The case of Ghent. *Information Polity, 21*(1), 5–19.
Wang, X., Hawkins, C. V., Lebredo, N., & Berman, E. M. (2012). Capacity to sustain sustainability: A study of U.S. cities. *Public Administration Review, 72*(6), 841–853.
Yin, R. K. (2018). *Case study research and applications: Design and methods*. Thousand Oaks, CA: Sage.
Zygiaris, S. (2013). Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. *Journal of Knowledge Economy, 4*(2), 217–231.

Patricia McKenna is the Founder and President of AmbientEase (Emergent Adaptive Solutions Everywhere), a Canadian company focused on smart cities and learning cities. Patricia is also the Director of the UrbanitiesLab, an initiative of AmbientEase. Patricia works within and across diverse domains of scholarship and practice (interdisciplinary) and collaborates in team efforts to set up international, national, regional, and local information services, research projects, startups, and other creative and future-oriented initiatives. Patricia engages across sectors with people around use experience and unexpected possibilities for leveraging and generating new relevancies and vibrancies in twenty-first century information spaces. Patricia holds a BA from the University of New Brunswick, an MLS from McGill University, and a doctorate in information management in the context of emerging technologies from Syracuse University.

Use of the Internet of Things in Public Governance for Law Enforcement and Inspection: The Case of Russia

Alexander Knutov and Evgeny Styrin

Abstract The Internet of Things is being actively introduced in Russian public governance for inspection and oversight. In this chapter, based on an analysis of IoT policy, legal acts, secondary statistical data, and the authors' own involvement in testing IoT technologies, we formulate cases and use them as a basis for an IoT classification oriented to the needs of government agencies. The spheres of application we consider are transport, justice, retail, and manufacturing. The case we study in greatest detail is that of the fur industry. We apply the method of cost–benefit analysis and examine the costs of using IoT in public governance to regulate the turnover of fur goods as well as the benefits for key stakeholders (government, society, business). We identify barriers that prevent IoT technology from being used effectively and describe the effects of implementing IoT in the fur industry and other areas in which IoT is used for inspection and oversight.

Keywords Internet of things · Law enforcement · Regulation · Inspection · Oversight · Effects · RFID technology · Fur industry · Tagging · Goods · Requirements · Counterfeit merchandise · Taxes

Abbreviations

GLN	Global Location Number
GLONASS	Global Navigation Satellite System
Goznak	Joint stock company "Goznak"
GS1	Not-for-profit organization "GS1"
GTIN	Global Trade Item Number
ICT	Information and Communication Technologies
IoT	Internet of Things

A. Knutov · E. Styrin (✉)
National Research University "Higher School of Economics", Moscow, Russia
e-mail: aknutov@hse.ru; estyrin@hse.ru

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_7

IT	Information Technologies
QR codes	Quick Response Code
RFID	Radio Frequency Identification
RFID tags	Control (identification) tags of items based on RFID technology

Introduction

Technologies today play a key role in transforming relations between government and business (Fountain 2001; Orlikowski 1992). By technological transformation in governance, we mean substantial changes in the ways government agencies exercise their powers and perform their functions (Gil-Garcia and Luna-Reyes 2008; Kraemer and King 2006). The researchers study the applications of ICT to public governance in order to identify success factors for ICT transformation (Criado et al. 2013; Heeks 2006; Klievink and Janssen 2009).

A spinoff topic is the impact of e-government, measured in terms of public value or direct economic profits or savings (Cordella and Bonina 2012; Jin and Cho 2015; Gil-García and Pardo 2005). For the purposes of our chapter, we consider the following potential economic effects of ICT implementation: budget savings in government functions and public services provision, increased investments by private stakeholders in government ICT infrastructure, and growth in exports in some industries.

Researchers and practitioners have used the term "e-government" to describe mainstream technological transformation projects initiated in public administration in the late 1990s in order to pursue ICT benefits (Janssen and Estevez 2013; Bertot et al. 2010; Dawes 2009). For the purposes of our study, we will use the term "digital government" to underline the transformative and innovative nature of ICTs when it is applied to government functions (Potnis 2010; Janowski 2015). We leave aside the internal organizational changes that can be caused by ICT and Internet of Things (IoT) in particular (Zuurmond 2005). The subject of our study is digital transformation of external interaction processes between government and stakeholders in the area of inspection and oversight.

We should also mention that digital transformation of government processes has to bring sufficient public value, which the World Bank (2016) calls "digital dividends." Government agencies gain new knowledge in policy making by involving citizens in problem solving and enabling them with data visualization maps and gaming and simulation tools (Janssen and Helbig 2018). The trend is for government policy to become totally data-driven and at the same time transparent and personalized to individuals and businesses (van Veenstra and Kotterink 2017).

The term "Internet of Things" was first used by Ashton (2015) to describe the ability of physical objects to exchange data through the Internet both with each other (Machine to Machine, M2M) and with human beings.[1] Fleisch (2010) defines

[1] Though the term "Internet of Things" became popular in 2010–2011, we refer to the important source by Ashton written in 2015.

IoT as a multilayered infrastructure consisting of relatively small hardware sensors that capture certain characteristics of the external world by generating machine-readable data and providing them to other nodes by means of Internet services. Fleisch (2010) points out the economic value of IoT, including the speed of transactions, product quality, and user behavior prediction.

Lu et al. (2018) paraphrase the European Commission's definition of IoT (Guillemin and Friess 2009) as "a dynamic global network infrastructure that will be integrated into and act as an extension of the future internet, in which various 'things' have unique identities, physical attributes, virtual personalities, and intelligent interfaces." So, in other words, "things" are an extension of the Internet fully identified and integrated at all layers—from physical to transport and logical—as is stated in the definition given by the ITU (2005). These definitions help us make the next logical step and state that new information systems will be dynamic, consisting of any real or virtual objects interlinked in accordance with the goals for which the information system was designed.

Lu et al. (2018) outline many directions and projects within each sphere of IoT application: infrastructural, organizational, individual, and comprehensive. We concentrate on the organizational direction—primarily on improving processes by means of real-time data monitoring as well as on saving resources and decreasing the reaction period (Atzori et al. 2010; Chen et al. 2014; Dlodlo et al. 2012).

The German government uses the term "Industry 4.0" to emphasize radical change in the automation of production processes as a result of the Internet of Things (EC 2017). The term "cyber-physical system," as an engineering system integrating computing algorithms with physical objects, has essentially the same meaning. Embedded computers and computer networks provide means of control and management over physical processes and usually interact through a feedback loop, where physical processes influence computations and vice versa (NSF 2017). In the case of the German government, the term "Industry 4.0" can be understood in a much broader sense than as just a cyber-physical system. It is also a strategy and national policy designed to provide small and medium-sized enterprises with IoT access and skills as a means of enhancing production efficiency and labor productivity.

Practical examples of cyber-physical systems with IoT sensors can be found in the area of computer network development and monitoring (Cisco), power grids (General Electric) and telecommunication networks and operations (Deutsche Telecom). In each case we view the company's surrounding ecosystem (Harrison et al. 2012) as a key stakeholder that has the capacity to collect, store, and analyze data from IoT sensors so that new models can be designed for predicting demand or providing more valuable services to other stakeholders in the ecosystem. The company's decision-making thus becomes data-driven (Brynjolfsson et al. 2011). We assume that the same type of ecosystem or cyber-physical system based on IoT infrastructure can be designed around public services and functions. In this chapter we will demonstrate the IoT ecosystem approach in the area of government inspection and oversight.

IoT technology allows an enterprise or government authority to collect and store large volumes of data about physical objects and human behavior. Due to the

decreasing price of data storage, companies and agencies can analyze data from the outside world in order to improve the quality of services and feedback (McKinsey 2015). McKinsey (2015) does not provide a detailed methodology, but estimates the economic effect of IoT implementation, emphasizing the ability to provide better services, save on internal expenses (e.g., personnel, energy), and save the client's time. The key industries for IoT implementation are healthcare, smart cities, industrial production, retail, transport, and housing and utilities.

WEF (2016) states that from 2009 to 2014 the price of sensors decreased by hundreds of times (from USD 30,000 to USD 80 per piece). This means that sensor integration in cyber-physical systems has become much less expensive, and the extent of IoT penetration is thus growing rapidly. WEF uses the term "Digital Value to Society (DVS)," which includes labor (job creation, salary growth), consumer benefits (time and cost savings), society and the environment (lives saved, carbon emissions, life expectancy). For the purposes of our chapter, we concentrate on consumer benefits and economic effects for individuals and businesses from inspection and oversight powers exercised by government authorities in certain areas of economic activity.

Our approach consists of an IoT evaluation and impact analysis which include key barriers to effective ICT (IoT in particular) applications (Heeks 2002). First, we describe some current applications of IoT in various areas of law enforcement in a Russian context, then we identify key IoT implementation barriers, and finally we calculate the economic impact of IoT on fur industry regulation in Russia. In our case study, we concentrate on the Russian federal government's regulation of commercial trade and public services and how this function is being transformed by IoT technology. We examine government information policy (Braman 2011) that supports the development of IoT infrastructure in Russia. We also look at the existing legal framework and observe technological changes in collaboration between Russian federal agencies and government-regulated businesses. Then we provide calculations of the economic potential of IoT applications. Finally, we explain the controversial nature of IoT as an ICT application by outlining institutional and organizational challenges involved in the practical implementation of IoT. In this chapter, we will limit ourselves to the applications of IoT in the area of law enforcement and inspection.

Method and Research Questions

The use of remote devices to transmit data to information systems in public administration may cause various both positive and negative social and economic effects. For example, IoT applications may minimize the number of on-site inspections and other visits to regulated entities as well as the quantity of regulatory bodies' reports. IoT allows for interaction with the government to be largely remote as well as more effective. At the same time, IoT technologies, like any other form of e-governance, may at times be misused and overused and thus cause ineffective and unreasonable

budget spending without creating value for stakeholders. The chapter aims to answer two research questions:

1. What effects can IoT technology have on government regulatory and law enforcement policy for stakeholders: society (citizens), state administration, and business?
2. What are the key barriers to the effective use of the Internet of Things in law enforcement and inspection practices?

Our *objective* is to study the impact of IoT technologies on public governance. First, we aim to determine the scope of IoT technologies as a guide to use in deciding whether one or another ICT application should be regarded as IoT. For this we develop a classification of IoT technologies. In order to develop an IoT technology classification, we identify and summarize actual cases in which IoT technologies have been used for law enforcement and inspection in Russian practice. We apply single-case design approach to a single unit of analysis: government inspection and oversight functions and powers exercised by means of IoT (Yin 1984). This method can be readily applied to new phenomena—in our case, IoT usage in public administration.

We selected the following spheres of IoT application, based on the actual implementation and launching of practical projects: transport, the fur industry, retail, the manufacture of alcohol products and environmental protection in a Russian context. We used the following sources of data to determine the spheres of IoT application and create case studies: (1) regulatory acts and official documents of Russian government agencies concerning the applications of IoT technologies in Russia; (2) official statistical oversight data as well as customs and judicial statistics; (3) the mass media, including specialized articles on IoT in business and IT publications as well as press releases by government agencies and materials posted on their official websites; (4) official data and data coming out of informal discussions with representatives of business associations and unions (the Russian Fur Union).

With the personal inclusion method, we drew on information systems available in the Internet (their user interfaces and public segments) that receive data from IoT sensors. We accessed these services as users and downloaded mobile applications that constitute the IoT software environment in order to study their functionality.[2] The use of multiple data sources and data triangulation (Patton 2002) ensures a more objective case study design.

Second, we select, from among the cases identified, a case appropriate for a study of the economic effect of IoT implementation: Application of RFID Technology in the Russian Fur Industry. We calculate the economic effect of IoT application by means of cost–benefit analysis. "Cost-benefit analysis is an important tool for the evaluation of the desirability of regulatory actions" (Revesz 2017). We used this method even though some researchers have concluded that "precise,

[2] For example, the following applications available in Google Play: Anti-Counterfeit Alco, https://play.google.com/store/apps/details?id=ru.fsrar.anticontrafact; Bill Checker, https://play.google.com/store/apps/details?id=ru.fns.billchecker.

reliable quantifiable" analysis is currently "unfeasible" (Coates 2015), since even the method's critics note that it may in any event be used as "a disciplined framework for specifying baselines and alternatives" (Coates 2015).

The study takes the method's limitations into account—particularly the fact that "the role of benefit-cost analysis is to provide information relevant to the decision, not to provide the decision" (Zerbe 1998). We applied the method of cost–benefit analysis to our case study of the fur industry, while at the same time applying the method of cash-flow analysis to additional tax revenues that the Russian Federation has received as a result of IoT use in the fur industry. The integrated use of both methods has been shown to be effective (Harlow and Windsor 1988).

The case study of RFID Technology in the Russian Fur Industry was supplemented with a study by the National Institute for System Study of Entrepreneurship, which covers key problems and criticism of the project as well as how respondents, including members of the business community, view the results of the project (Shevernev 2016). We assume that cost–benefit analysis in this case study is very important, since it complements a previous sociological study of the opinions of multiple project stakeholders. Besides cost–benefit analysis we determine the reasons for the adoption of IoT technologies in fur industry inspection and oversight in Russia, describe the IoT technology used, benefits obtained by each stakeholder group in the project and problems encountered as well as criticism of the project.

Third and last, we summarize the data obtained from a cross-analysis of case studies and identify the key barriers for the effective use of IoT technologies in law enforcement and inspection.

IoT Applications and Classification of IoT Devices and Sensors Used for Law Enforcement in Russia

Based on definitions of IoT (Ashton 2015; Fleisch 2010; Lu et al. 2018), for the purposes of this chapter, IoT technology will include ICT applications meeting the following criteria: they must be government-regulated physical objects ("things") containing embedded technologies for interaction with each other or the external environment[3]; the devices (objects) used must be automatically identifiable in information systems; the devices must contain machine-readable data that they have collected on the external environment or transform such data into machine-readable formats; the devices must have machine-to-machine capability. The automated transmission of data by wireless and wired networks to a variety of information systems is not regarded as an essential criterion of such devices. Figure 1 is a schematic illustration of IoT technology meeting the given criteria.

[3] This feature corresponds to the definition of IoT in the Gartner IT Glossary (2012): https://iq.hse.ru/news/199111386.html (accessed August 4, 2017).

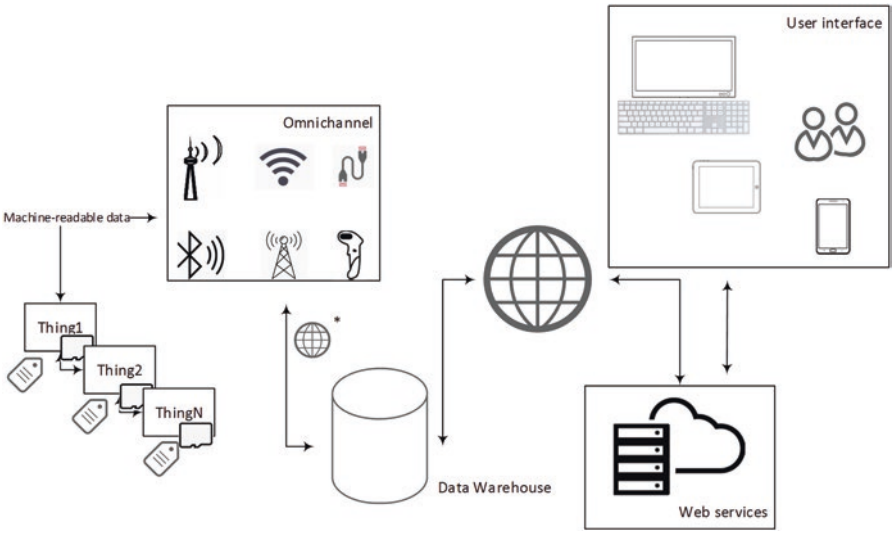


Fig. 1 IoT architecture. ∗ The automated transmission of data by wireless and wired networks to a variety of information systems is not taken into consideration

Table 1 Applications of IoT technology in Russian public governance

Sphere of application	Purpose	Objects involved	Examples
Law enforcement	Recording and monitoring, inducing individuals and legal entities to comply with statutory requirements	Individuals, legal entities, entrepreneurs and their activities	Trade equipment connected with information systems of the regulator
Smart cities	Urban management	Urban infrastructure	Smart traffic lights
Socially significant monitoring	Protection and study of the environment, identification of factors unfavorable for the public, prevention of emergency situations	The environment, natural factors and phenomena	Online air pollution sensors

The Internet of Things is used with increasing frequency in Russian public governance. Public administration cannot ignore the rapid strides being made by ICT and is increasingly using IoT. In Russia, IoT technologies (in the sense indicated above) are used for public governance in the following areas: (1) law enforcement efforts by government agencies to induce legal entities and individuals to comply with statutory requirements and maintain better records of their activities; (2) urban services, for example, the development of Smart Cities, regulation of traffic, parking, municipal utility vehicles and public transport, and so on; and (3) various kinds of socially significant monitoring, for example, observation of natural, seismological, and geophysical phenomena, environmental monitoring (the use of Internet sensors to continuously measure the level of air pollution, etc.). Various applications of IoT technology in these areas are outlined in Table 1.

The present study focuses on the use of IoT for law enforcement only. The other two areas do not have any special distinguishing features in terms of IoT use and do not differ from similar commercial uses for services and monitoring. IoT technology is assigned an important role in the ongoing reform of state inspections in Russia. The government's strategic goal is to equip regulated entities, wherever possible, with devices allowing government-regulated business parameters to be transmitted in real time to government information systems by mobile networks. The passport of the priority program for reform of control and oversight[4] envisages the widespread use of such technology in public governance by 2019, and this will require legislative amendments. Even before these innovations take effect, however, a number of government regulators in Russia have already acquired experience with IoT technology.

Before reviewing cases of successful IoT adoption in public administration specifically in inspection and oversight, we first provide below a classification of IoT. This classification is based on an analysis of cases involving the use of IoT in various Russian industries (areas) for purposes of law enforcement and inspection: (1) use of means of identification whereby machine-readable data on regulated entities can be automatically processed based on readings using optical, radiofrequency or other information technologies (from simple barcodes and QR codes to more sophisticated RFID tags) ("automatic means of identification"); and (2) use of sensors and devices that automatically record the parameters of regulated business activity and transmit data by wireless or wired networks to government information systems ("automatic sensors"). Automatic sensors differ from automatic means of identification in that they not only store manually or automatically entered data on objects, but can independently record the desired parameters of objects and the external environment and generate machine-readable data to be subsequently transmitted to any information systems. Then, automatic sensors and devices may be subdivided into two. Devices installed at sites belonging to regulated entities and so used to inspect the activities of only those entities ("personalized devices"). And, devices installed in public areas and used to inspect the activities of an unlimited number of entities in those areas ("nonpersonalized devices")."Automatic sensors" also include a subgroup of devices that automatically locate regulated objects via a global positioning system and transmit geolocation data in real time to government geoinformation systems ("geonavigation devices"). Figure 2 and Table 2 show our classification of IoT applications for law enforcement and inspection in Russian public governance.

Next we will briefly review IoT application case studies based on the above classification. The cases are grouped in accordance with the classification.

[4] Priority Program for Reform and Oversight (approved by the President's Council for Strategic Development and Priority Projects, 2016), http://government.ru/news/25930/ (accessed July 4, 2017).

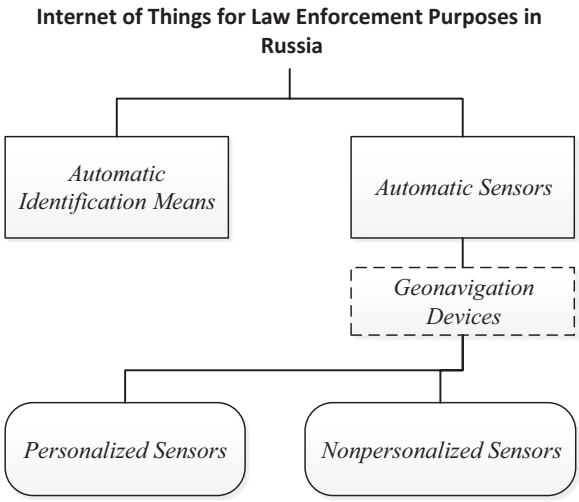


Fig. 2 Classification of IoT applications for law enforcement and inspection

Table 2 Classification criteria for IoT applications in law enforcement and inspection

IoT application for law enforcement and inspection	Recorded data	Ability of devices to automatically record and generate data	Objects involved	Examples
Automatic means of identification	Identifying and descriptive features of any objects	No	Any things on which machine-readable data is required	Microchips to identify goods, pets and other objects
Personalized devices	Any data on the functionality of any objects	Yes	Any objects equipped with personalized devices that continuously monitor their functionality	Devices that monitor the functionality of equipment for the production of alcohol and spirits
Nonpersonalized devices			An unlimited number of people and moving objects in a device's area of operation	Video surveillance devices that capture traffic violations and violations of public land
Geonavigation devices	Geonavigation data	Yes	Any objects equipped with personalized devices for continuous geonavigation monitoring	Online tachographs

Automatic Means of Identification

In recent years, mandatory item-level tagging has been introduced in Russia for certain types of products, involving scannable QR codes and barcodes, and/or radiofrequency identifiers containing detailed product information (radio tags, chips). Such products include, for example, alcohol products and natural fur clothing. Each bottle of alcohol in Russia, for example, is identified by a QR code in the Unified State Automated Information System. The product record in the system includes the entire history of how a given bottle came to be on store shelves (its manufacturer or importer, distributor, retailer, etc.). Members of the supply chain (manufacturers, importers, wholesalers, and retailers) who fail to enter product information in the system can be fined USD 2500–3300. Buyers can use a special mobile application to check the legality of purchased alcohol by scanning the QR code on the bottle or sales receipt.

Such technologies for automated product tracking are expected to steadily gain currency. A pilot project to tag pharmaceuticals was launched in 2017, and the potential use of such technologies for salmon products, fine woods, and animal foodstuffs (sausage, canned goods, dairy products, etc.) is under consideration. A draft federal law that is currently under development—"On the Labeling of Goods with Control (Identification) Tags in the Russian Federation"—will set unified guidelines. Below, the effects of such measures will be studied by examining a case study of the tagging of fur products.

Automatic Personalized Sensors

Applications of automatic personalized sensors for law enforcement and inspection in Russia are outlined in Table 3. In speaking of the effects of such technologies, it should be noted that they allow regulators and regulated entities to collect relevant

Table 3 Applications of automatic personalized sensors for law enforcement and inspection in Russia

Sphere of application	Location of sensors	Data read and transmitted to government information systems
Retail trade	Point-of-sale equipment (including online stores)	– sales information for tax purposes – electronic sales receipts
Manufacture of alcohol products	Manufacturing equipment for alcohol and spirits	– output (in liters and number of bottles) – alcohol content of finished products
Industrial manufacturing that pollutes the environment	Stationary sources of air and water pollution	– quantities of air and water pollutants released and the concentration of pollutants (from 1 January 2018)
Judicial proceedings	Suspected or charged offenders under house arrest during a criminal investigation (wrist bracelets)	Data on the location of individuals (geonavigation data) If an individual goes beyond a certain distance (determined by the rules of house arrest—generally 50–100 m) from a fixed receiving unit, the devices notify the corrective services information system

information based on objective (verifiable and registered) data and without being a drain on government or private resources. The only expenses required are for the initial installation and periodic maintenance of sensors.

For example, the real-time transmission of data on sales and payments allows the Federal Tax Service to obtain accurate tax information and automatically identify violations and risk areas where audits can be specifically targeted for greater effectiveness. Such technology also allows the public to perform control functions. The concentration of data on payment transactions enables the tax service to use big data technologies and thus make its governance solutions more effective. The new technology is expected to minimize the need for tax audits of retailers, since the retail business will be completely transparent to tax authorities. It is too early to measure the real success of such innovations, since the system only went into operation on 1 July 2017.

The effects of automated personalized sensors can be assessed, however, in the case of electronic bracelets worn by suspected and charged offenders under house arrest. This IoT technology has been in use since 2011 and has reduced the number of cases in which criminal suspects are confined. Now investigators can be assured that a suspect will not go into hiding before the investigation is concluded, and this can be done in a more humane manner without resorting to arrest and confinement. Figure 3 shows statistics on the use of house arrest as a pretrial restraint during criminal investigations (Soloviev 2010; Statistics Database of the Judicial Department under the Supreme Court of the Russian Federation 2011).

The increasingly frequent use of house arrest since 2011 has to do with the introduction in that year of electronic bracelets to monitor suspected and charged offenders. Traditional methods of monitoring persons under house arrest—on-site (visual) inspection by law enforcement authorities—are costly for the state, and limited

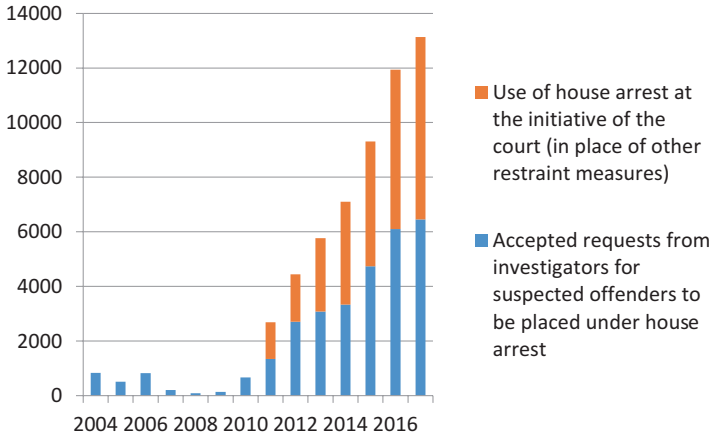


Fig. 3 Judicial statistics on the use of house arrest as a pretrial restraint

resources meant that such pretrial restraints were rarely employed. The new technology has enabled far more frequent use of house arrest instead of confinement for suspected and charged offenders. There is no doubt that, without this option, tens of thousands of people who have been placed under house arrest since 2011 would have been confined for the duration of the investigation (i.e., before their guilt was established).

Automatic Nonpersonalized Sensors

Automatic nonpersonalized sensors are largely means of automatically capturing violations—above all, traffic violations—on film and video. This technology has been familiar for some time and comes under the heading of IoT insofar as traffic enforcement cameras automatically transmit machine-readable data on the external environment (the vehicle's license number and the circumstances of the violation) to information systems, making it possible for violators to be ticketed automatically, without human involvement.

Aside from traffic enforcement, Russian law also allows the video surveillance of public land, but this application has not yet gained wide currency and is found in only some constituent entities of the Russian Federation.

Geonavigation Devices

Since 2008, Russian law has increasingly required that vehicles in certain categories be equipped with geonavigation devices. Such devices are now mandatory for buses used in commercial transport (with seating for more than eight); buses used for the organized transportation of groups of children; vehicles transporting special, hazardous, oversize and/or overweight loads; and garbage trucks. The idea—for these devices to transmit machine-readable navigation data in real time to government geonavigation systems—has so far been put into practice in only some constituent entities of the Russian Federation.

Russian law also calls for trucks (with certain exceptions) to be fitted with tachographs to monitor observance of the speed limit as well as drivers' work and rest requirements. Tachographs qualify as geonavigation devices because they have an external antenna to receive signals from the GLONASS and GPS satellite navigation systems as well as a communications module for transmitting geonavigation data to external information systems via mobile networks. Essentially, everything needed for the automatic online monitoring of drivers' work/rest regimen is already in place, but the system today is still in sleep mode.

Geonavigation devices include special onboard devices installed on heavy trucks (with a maximum weight of over 12 tons). National law requires the owners of such vehicles to compensate for damage to the roads. Road mileage is measured by these onboard devices while a vehicle is in motion, and charges are calculated based on the data they automatically transmit online. The onboard devices use global positioning

systems and generate machine-readable data on the route traveled. Such data are automatically transmitted to a special information system that uses them to calculate the fees a truck owner will be charged for the use of road infrastructure.

Trucks transporting ethyl alcohol must be additionally fitted with geonavigation devices that automatically track their movement and transmit data on their current location, the route traveled and the times and places of stops to an automated monitoring system via global positioning systems. The requirements prescribed by Russian law for fitting trucks with geonavigation devices are thus unsystematic, and trucks may have as many as three onboard devices in operation, some of them useless, since the government does not yet have information systems in place capable of receiving geonavigation data. Meanwhile, statutory requirements that vehicles be equipped with such onboard devices have already gone into force. As a result, the devices have been criticized in Russia as ineffective.

The use of IoT technologies for geonavigation has not yielded any notable results. Effective use should have allowed transport inspectorates and traffic police to reduce the number of traditional inspections as a result of automated control. Another such effect would have been a reduction in the number of traffic accidents involving death or injury because drivers and transport company employees better complied with speed limits, drivers' work/rest regimen and other rules.

This case is nonetheless important for our study, because it demonstrates that uses of IoT technologies are not all equally effective. In this case, an analysis of regulatory documents showed that the use of IoT was ineffective because regulation outstripped the level of technology in the regulated area and the ability of the regulator (the Federal Transport Inspection Service) to incorporate information technologies. Companies were required to use IoT prematurely, when the required infrastructure was not yet in place.

Application of RFID Technology in the Russian Fur Industry

Following our overview of IoT technologies used in Russia for law enforcement and inspection, we will now take an in-depth look at **a case involving the mandatory use of RFID tags for natural fur clothing**. This case lends itself to the method of cost–benefit analysis and allows us to determine the costs and benefits for key stakeholders, since the technology was introduced relatively recently and we can do a "before and after" comparison. *The reason for additionally regulating* fur products was the large extent of illegal trade and the resulting profusion of counterfeit merchandise on the market.

Research data put out by the Higher School of Economics (National Research University) (Radaev 2016) show that 97% of fur products illegally imported into Russia come from China, 66% from the European Union and Turkey and 26% from countries of the Eurasian Economic Union.[5] Illegal imports of fur products include

[5]The Eurasian Economic Union (EEU) is an integrational political and economic project for five post-Soviet countries: Russia, Kazakhstan, Belarus, Kirghizia, and Armenia.

cases in which false declarations are submitted for purposes of evading customs payments and value-added tax. Fur clothing is thus imported under other headings as products that qualify for lower duties.

China, as Russia's chief supplier of natural fur clothing, accounts for over 90% of such illegally imported merchandise. As a result, the state loses revenue from taxes and levies, consumers have no assurance of product quality, and law-abiding market players are unable to compete with the prices offered by sellers of illegal merchandise.

To address these problems, it was proposed that a system based on RFID tagging be used to track the turnover of fur products. The system went into operation on a voluntary basis on 1 April 2016 and became mandatory on 12 August 2016. Mandatory tagging became possible once all member countries of the Eurasian Economic Union had ratified the agreement for a pilot project in 2015–2016 to introduce control (identification) tags for commodities under the heading "Articles of clothing, clothing accessories and other commodities of natural fur" (Grodno, 8 September 2015).

The technology involved in tagging fur products is as follows: All members of the supply chain—manufacturers, importers, distributors (wholesalers) and retailers (including secondhand stores)—must join the tagging system by either (1) entering into an agreement for the supply of control (identification) tags: RFID tags involving elements of secure printing (such tags are produced only by the state company Goznak); (2) joining GS1 and obtaining a GLN code (the tagging system is based on an international system of standardized recording and barcoding of logistic units and makes use of three international codes: GLN, GTIN, and SGTIN)[6]; (3) obtaining access to the State Commodity Tagging System; (4) obtaining a reinforced qualified electronic signature for interaction with the State Commodity Tagging System; or (5) purchasing an RFID reader and printer.

After all these steps have been completed, the tagging process can begin. This involves generating a Global Trade Item Number (GTIN) linked to all relevant information on the trade item, recording all of this information on the tag, transmitting the information to the Commodity Tagging System and, finally, affixing the tag to a fur item. Each subsequent member of the supply chain (except for the end consumer) checks the item upon receipt, updates the information on the tag, adding its own identifier, and transmits this information to the Commodity Tagging System. The following commodity information must be entered in the tagging system: full name; brand/trademark (where applicable); manufacturer (legal entity or individual entrepreneur); country of origin; commodity code in the Eurasian Economic Union's Foreign Trade Commodity Classification; size; type of fur; dye information; style; color; and date and number of declaration of compliance. All members of the supply chain provide their taxpayer identification numbers when entering information in the Commodity Tagging System.

[6] Website of the Organization on Standardization: https://www.gs1.org/.

Product turnover thus becomes almost completely transparent for both regulator and consumer. It is possible to access exhaustive information on an item and its legal status in a given store at any point in time. RFID technology allows such checks to be done automatically by means of radiofrequency sensors in logistics warehouses, for example, or customs checkpoints. Such checks can also be done by end consumers, enabling applications in law enforcement and inspection as well as crowdsourcing.

Enforcement

Violators of the new tagging rules may be fined up to RUB 300,000 (USD 5000), with the goods themselves being seized and destroyed (Article 15.12 of the Administrative Offenses Code of the Russian Federation). In the case of large shipments worth upwards of RUB 1,000,000 (USD 17,000), criminal charges may be brought under Article 171 of the Russian Criminal Code, and convicted offenders, in addition to having their goods seized, may be fined up to RUB 1,000,000 and face a prison sentence of up to 6 years.

The results of the project have been as follows: As of the beginning of 2017, according to the Russian Fur Union, over 8500 users had been registered in the system, over 6.7 million tags had been ordered, and 3,800,000 fur products had been tagged.[7] For the first time, in effect, the government found out how many companies were trading in fur products and what quantities were involved. Prior to this, no reliable data had been available. According to the Russian Ministry of Industry and Trade, 973,000 trade items, worth more than RUB 55 billion, were brought back into legal circulation, and customs payments for such merchandise were up 40%.[8]

Official foreign trade statistics show that the turnover of fur products did, in fact, increase in money terms in the fourth quarter of 2016 and the first quarter of 2017 (up 55% since 2015 and 2.3% since 2014).[9] The timeframe is still too short, however, to assess the degree to which this project has been a factor in boosting the legal turnover of fur products. No further data are as yet available, but the fact that this growth comes during an economic crisis, when consumer demand in Russia and real incomes are declining, does encourage us to see this project as the reason.

---

[7] Results of Fur Production Tagging, Report (2017), Russian Fur Union, http://www.rpms.ru/index.php?option=com_content&view=category&layout=blog&id=1&Itemid=10&lang=ru&limitstart=18 (accessed August 18, 2017).

[8] Materials from a meeting of the Government Commission for the Prevention of Illegal Trade in Industrial Products, http://minpromtorg.gov.ru/press-centre/news/#!itogi_provedeniya_veernyh_ispytaniy_tovarov_obsudili_na_zasedanii_goskomissii_po_protivodeystviyu_nezakonnomu_oborotu_promyshlennoy_produkcii (accessed July 10, 2017).

[9] Calculations are based on data from the Russian Customs Statistics Database: http://stat.customs.ru/.

Another trend should also be noted. Some companies, instead of going legal, have adopted a strategy of closing up shop. According to a study by the National Institute for System Study of Entrepreneurship, whose findings were presented at the international forum Anti-Counterfeiting 2016 in Yerevan (Armenia), the number of companies that decided to liquidate their fur goods business between August and October 2016 was sharply higher than in the same period of 2015: 122 companies in 2016, up from 71 companies in 2015—a 72% increase (Shevernev 2016). Regardless of that fact, the turnover of fur goods increased.

Seventy percent of market players surveyed for the National Institute's study had a favorable opinion of the new system of mandatory tagging.[10] As the chief reason for this opinion, they cited the elimination of noncompetitive advantages enjoyed by illegal business.

Project costs should be divided into business costs and government costs. Business costs are shown in Table 4. Government costs—those involved in setting up the State Commodity Tagging System—totaled almost RUB 600 million (USD 10 million) in 2016–2017.[11]

The benefits of the project should be assessed for three stakeholders: society, government and business. *Society (consumers)* has benefited from greater assurance that fur goods come from the stated manufacturer and are of the stated quality. Other factors of importance for consumers have been unaffected. According to federal statistics, consumer prices for natural fur clothing have remained virtually unchanged.

The government has benefited from higher customs and tax revenues as a result of growth in the legal turnover of fur products. We have already cited customs statistics. Trade in fur products in the period after the project was realized—from the first quarter of 2016 through the second quarter of 2017—came to USD 93 million: USD 33.2 million higher than in the same period of 2015–2016 and USD 2.1 million higher than in the same period of 2014–2015. Given an average growth in turnover of USD 17.65 million and a 10% rate of customs duty on imported natural fur products, it turns out that the government collected an additional USD 1.8 million (RUB 108 million) in customs payments in a 6-month period. Assuming this level of additional customs revenues on an annual basis, the government will fully recoup its investments 3 years after the start of the project. And if we keep in mind that the state-funded Commodity Tagging System is also to be applied to commodity groups other than fur products, the government's investments can be judged cost-effective.

[10] The survey was conducted by the National Institute of System Research on Entrepreneurship Problems (http://e.ru/) in October, 2016, by means of a questionnaire. The 300 respondents represented businesses that produce, import and trade in clothes, including fur products, in seven Russian regions, including Moscow, St. Petersburg, and Tatarstan. The survey's findings were not officially published but were presented at the international forum "Anti-Counterfeiting 2016," Yerevan, Armenia.

[11] According to data of the Russian National Integrated Public Procurement System (procurement notices 0173100007817000006, 0173100007816000051, and 0173100007815000103).

Table 4 Costs incurred by players on the fur goods market that implement tagging technology

Cost type	Unit cost	Number of market players/fur products	Total nonrecurring costs	Total annual costs
Purchase of RFID printer and RFID reader	RUB 40,000 (USD 670) and up	8500 companies	RUB 340,000,000 USD 5,670,000	–
Obtaining a reinforced qualified electronic signature	RUB 5000 (USD 83)	8500 companies	RUB 42,500,000 USD 708,000	–
GS1 membership	25,000 (entry fee); 15,000 (annual dues)	8500 companies	RUB 212,500,000 USD 3,542,000	RUB 127,500,000 USD 2,125,000
Ordering tags from Goznak	RUB 22 per tag, excluding delivery	~800,000 tags		RUB 176,000,000 USD 2,933,000
Labor time involved in processing and affixing tags and transmitting data to the State Commodity Tagging System	0.25 of the rate in one company ~RUB 9000 per month (salary), ~RUB 2700 in payroll taxes	8500 companies		RUB 1,193,400,000 USD 19,890,000
Total:	RUB 595,000,000 USD 9,917,000	~RUB 1.5 billion ~USD 25,000,000		

Source: the authors' calculations

It is hardest to assess the project's *benefits for business*. As we have noted, the project has not resulted in higher consumer prices for fur goods (other than growth attributable to inflation). Price growth might have been expected as the market rid itself of unscrupulous players that evaded customs duties and value-added tax. So far, this has not been the case, however, and it could thus be said that business has not as yet benefited. At the same time, as we have indicated, business is positive about the project's results. The National Institute for System Study of Entrepreneurship, in its survey of 300 representatives of the fur industry, found that this favorable opinion has to do with the factors indicated in Fig. 4.

Thus the chief benefit for business was that "gray" operators were driven out of the market. It is extremely difficult to compete with players who deal in counterfeit goods because they pay less tax and are able to price their goods lower. The tagging system created a level playing field for all.

Problems in Implementing the Project

The government and players on the fur goods market encountered a number of problems in implementing the tagging system. Eighty-six percent of those who responded to the survey conducted by the National Institute for System Study of Entrepreneurship experienced problems in implementing the tagging system.

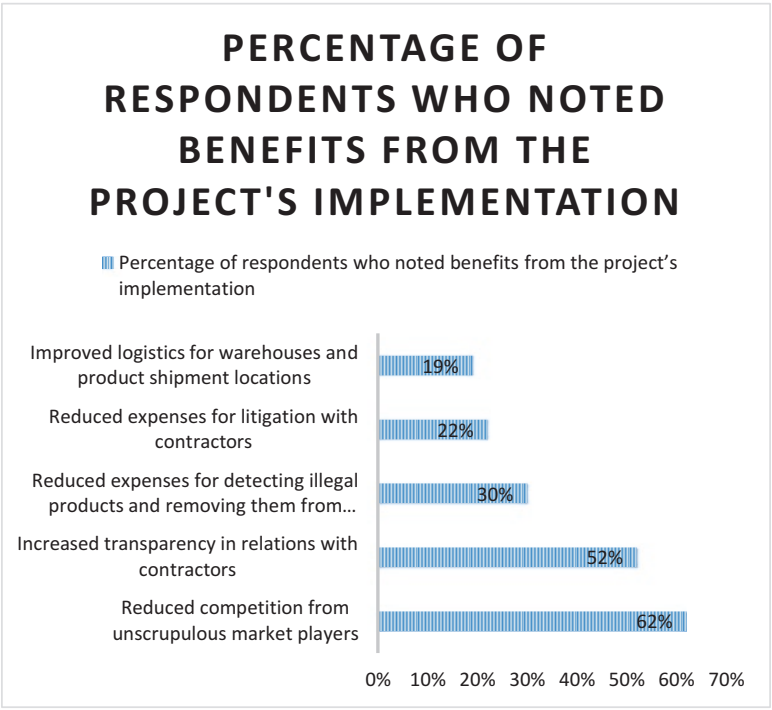


Fig. 4 Findings of a survey of representatives of the fur goods market (percentage of respondents who noted benefits from the project to tag fur goods). (Source: National Institute for System Study of Entrepreneurship (survey findings presented at the Anti-Counterfeiting 2016 international forum in Yerevan, Armenia))

Of these, 25% had to suspend project implementation for a month or more. Respondents most frequently noted technical problems involved in implementing the project. In particular, according to project rules, tags cannot be issued to companies that owe taxes and levies, but it turned out that many companies had a "technical" debt of only a few rubles (cents). They were denied tags on formal grounds and could not continue doing business. They had to suspend all transactions until such debt issues were resolved. Respondents also noted that the supplier of RFID tags (the state company Goznak) failed to deliver tags on time. The delays forced companies to cease business until they received the tags they had ordered, and this naturally entailed operating costs.

Respondents also mentioned a problem with defective tags. Up to 10% of the tags in each delivery were defective. Such tags were unusable and had to be reordered. At the same time, a larger number of tags than needed were ordered due to the possibility of defects, and this also entailed unnecessary costs. There were also cases in which RFID tags malfunctioned after being affixed to articles of clothing.

Finally, respondents noted that the Commodity Tagging System, Goznak's website and GS1Rus information resources sometimes malfunctioned. There were periods when information systems could not be accessed or failed to respond and users were unable to operate them. It was impossible to register, send an order, and so on.

These problems, however, are technical and easily eliminated. Such problems can occur at the start of any new project. Some criticism of the project, however, involves more conceptual issues relating to the chosen methods of governance. The project was criticized for being too complex and over-regulated. Companies have to interact with three parties: the tax service, Goznak and the international association GS1. The fact that the government essentially requires companies to join GS1 has drawn particular criticism. This entails membership fees, as mentioned earlier, and project participants have to obtain GLN and GTIN numbers from GS1, since the Commodity Tagging System is based on an international system of standardized recording and barcoding of logistical units. Critics of the project say that nothing prevents a tagging system from being based on public protocols that are free of charge for project participants. RFID technology can operate with GS1-compatible codes, as confirmed by manufacturers of the relevant equipment. In effect, the situation as it is restricts competition.

Some question the need for RFID tags in the first place. All required information on an item could be encoded in a simple two-dimensional barcode, making the project substantially less expensive. Companies would not have to purchase RFID tags (at a cost of RUB 22 each, plus shipping) or costly equipment for reading them. Two-dimensional barcodes can be printed out on a printer and do not have to be ordered. Others, however, argue that without RFID technology, the project loses the advantage of automated processing and inspection at logistics warehouses and customs checkpoints.

It can thus be said that the project's failings include requiring businesses to use complex and costly technologies with capabilities that go beyond the project's objectives.[12] The supply chain for RFID tags was not fully worked out before the project was implemented. Insufficient attention was given to the quality of RFID tags, resulting in defective output. Moreover, the selected technology forced businesses to pay for the services of outside entities, which could restrict competition.

Prospects for Further Development of the Project

Looking ahead, there are plans to apply the Commodity Tagging System to other groups of commodities. A pilot project for the tagging of pharmaceuticals is already underway on a voluntary basis, and there are plans to begin tagging footwear. Regulators should be guided by the following considerations in selecting goods to be tagged. There should be a substantial proportion of counterfeit merchandise on the market or of merchandise that is widely involved in illegal import schemes.

[12] We should note that this is the opinion of respondents who do not want to pay for costly RFID technology and believe that the project's objectives could have been achieved with simple two-dimensional barcodes. The project's defenders, however, believe that RFID technology can make warehouse logistics more effective in addition to fighting counterfeit goods. We will note only that increasing the effectiveness of warehouse logistics was not an objective of the project, and businesses that so desired could have introduced the technologies voluntarily rather than being required to use them.

Also, the retail cost per unit should be relatively high (so that tagging costs are not a large component of the cost of a commodity). Finally, a substantial proportion of merchandise should be imported for domestic consumption (since it is hardest to ensure the legality of imported goods). A draft federal law that is currently under development—"On the Labeling of Goods with Control (Identification) Tags in the Russian Federation"—will establish unified guidelines and tagging technologies and determine the range of goods to which tagging requirements will apply.

IoT's Effects on Government Regulatory and Law Enforcement Policy

The cases we have reviewed allow us to state how government, business, and society may be affected by the use of IoT in government regulatory and law enforcement policy. Government should enjoy enhanced effectiveness in inducing individuals and organizations to comply with requirements. "Effectiveness" here may be understood as either maintenance of the same level of law and order as before IoT was introduced, but with substantial savings of resources (human, material), or a substantial reduction in the number of violations and cases of damage to protected assets after the introduction of IoT, with the same level of resources spent on maintaining order. In fiscal areas, the government can count on higher receipts of taxes and other mandatory payments because of the greater discipline of taxpayers regulated by IoT.

Business can expect reduced costs for interaction with the government, including inspections and report filing, due to automated control. Another important factor is the creation of a level playing field for all market players, which is not the case when inspections are selective. Regulation of business will become objective and comprehensible, and it will have 100-percent coverage. The principle of certainty of punishment for unscrupulous market players will be realized.

Society can rely on a higher level of security in regulated areas because of more responsible and law-abiding behavior on the part of economic entities and can also expect more effective use of public funds collected from taxpayers.

Key Barriers and Recommendations for Further IoT Implementation in Government Regulatory and Law Enforcement Policy

Based on the cases reviewed, we can list key barriers for further IoT implementation in government regulatory and law enforcement policy. Barriers that may result in unsuccessful use of IoT and create a situation in which stakeholders' costs outweigh benefits can be divided into three groups: technical, governance, and/or economic.

Technical barriers are errors in the system's design that cause IoT malfunctioning and lack of coordination between those involved in introducing and using IoT. Such problems may arise in any area of activity and are not specific to IoT.

Governance barriers to the successful use of IoT include implementing IoT before making the appropriate changes in administrative procedures and without eliminating human involvement from the regulated actions and operations. In other words, IoT is used in addition to existing controls, rather than replacing them, which can result in redundant means of regulation. Governance errors also cover cases in which regulators require the use of overly complex and costly technologies with unnecessary technical capabilities, when the goals of law enforcement and inspection can be achieved by simpler and less expensive means. Another governance error is to require the use of IoT prematurely, when the required infrastructure is unready and the IT environment needed to process machine-readable data from IoT sensors and devices is not yet fully formed.

Finally, economic barriers to the effective use of IoT include cases in which competition is restricted and regulators can impose the products and services of specific persons and companies when IoT is used for public governance (hardware or software required for communication and IT interaction that is available from only one manufacturer and/or seller).

To rule out such problems, the authors propose that the following recommendations be followed when IoT technologies are used in law enforcement. Before society or business is required to use sensors and devices, an economic analysis should verify that the potential benefits outweigh the costs involved in introducing and applying the new technologies for the government, businesses, and individuals. When IoT technologies are implemented for law enforcement and inspection, current processes of governance must be modified with a view to eliminating human involvement in some processes and operations. In applying IoT technologies, regulators should ensure that competition is maintained and that individuals and organizations are not required to use the services or products of a single company. Even if services or products are currently offered by only one company, regulators should make sure that offers by other interested persons and companies are still possible. Before a decision is made to require businesses or individuals to use automatic devices and means of identification, the infrastructure for automated processing of data from such devices must be fully operational. Parallel implementation can result in situations where devices operate to no purpose, as is the case with the geonavigation devices required for trucks in Russia.

Above all, IoT technologies should make it easier, not harder, for law-abiding businesses to operate and for government agencies to carry out inspections and enforce the law. These recommendations apply to law enforcement officials who are implementing government projects to introduce IoT technologies. If the recommendations are followed, the Internet of Things can greatly facilitate law enforcement and inspection and be more effective in inducing individuals and organizations to comply with the law than traditional practices of governance (inspections, collecting reports, etc.). IoT reduces law enforcement and inspection costs for both government and business.

Limitations and Future Research

Our analysis of the use of IoT in the Russian public sector has certain research limitations. First, the use of IoT in the public sector was analyzed within the narrow scope of law enforcement and inspection. Uses of IoT for municipal services and environmental monitoring remain beyond the scope of our research.

In our view, the use of IoT for law enforcement and inspection is of particular interest for researchers studying public governance and its effectiveness. For one thing, a new stakeholder comes into play when IoT is introduced: persons whose activities are regulated using IoT. What is more, this use of IoT has been the subject of very few studies, unlike the use of IoT in smart cities (van Waart et al. 2016; Anthopoulos et al. 2016).

The case study method involves a number of limitations. First, we studied only one case in detail and applied the method of cost–benefit analysis to that case. Other cases were used to form an overall picture of how IoT is currently used in Russian law enforcement and inspection—specifically, to create a classification and determine the boundaries of IoT use. In this connection, "single-case designs" are better rather than "multiple-case designs," as these are understood by Yin (1984). Based on our detailed case study of the fur industry, we were able to formulate the key barriers and recommendations for further IoT implementation in government regulatory and law enforcement policy.

Second, it should be noted that, in applying the method of cost–benefit analysis to IoT in the fur industry, we analyzed only economic factors, such as additional costs and revenues for business and government as a result of the introduction of IoT technologies as well as benefits of an economic nature (the enhancement of competition, for example). Our study does not address the impact of IoT on the welfare of society or on environmental protection and the conservation of species. These effects are difficult to measure and do not lend themselves well to our chosen method of cost–benefit analysis. Although it is common to evaluate noneconomic factors in a cost–benefit analysis (Zerbe 2004), the authors have set these issues aside for future research.

In addition, further research on the impact of IoT technologies on public governance can be done in the following areas: an economic assessment of IoT's actual impact on business in terms of rising or falling costs for the mandatory implementation of such technologies; analysis of the optimal level of use of IoT technologies and capabilities for law enforcement and inspection—a level that is sufficient without involving any redundancy; a study of security issues affecting data from IoT devices and sensors with a view to preventing violations of privacy and confidentiality and protecting against misuses of such data; and protection of competition when technologies are used for IoT solutions in the public sector. This last area of research is relatively independent and was not addressed in this chapter. It should be emphasized, however, that the government, in collecting data from automatic devices, must guarantee the security of personal data, commercial secrets and other information protected by law.

Conclusions

Our overview of IoT technologies used in Russia for law enforcement and inspection and our in-depth look at a specific case lead us to the following conclusions. We assume that our scheme drawn from Russian experience is an optimal classification of IoT technologies currently used for law enforcement and inspection. We selected cases involving the use of IoT to test this classification and found the classification to be justified and sufficient. The uses of IoT that we have considered (one in detail) allow us to answer the questions posed in our study. We found that IoT technology had the following effects on government regulatory and law enforcement policy: economy of resources used for law enforcement and control, greater effectiveness in inducing individuals and organizations to comply with requirements, and a higher level of security in regulated areas of activity.

At the same time, our study identified cases in which IoT technologies are not used effectively enough. For example, requirements that vehicles be fitted with various geonavigation devices in Russia are unsystematic, inconvenient for vehicle owners and involve unjustified costs. They do nothing to facilitate law enforcement and inspection. Moreover, satellite navigation equipment and tachographs still operate to little or no effect. In most cases, navigation data from such devices are not transmitted or processed by government geonavigation systems. Based on our analysis of the uses made of IoT in Russia, we listed key barriers involved in introducing IoT for law enforcement and inspection: the high cost and unnecessary complexity of the required technologies, technical problems involved in implementation, and potential restriction of competition.

To avoid these problems, we have developed a set of recommendations to be followed for the appropriate and effective use of IoT technologies in law enforcement: prior economic analysis (regulatory impact assessment) of the proposed technologies, reengineering of administrative procedures to eliminate human involvement in some processes and operations, adherence to the principles of protection of competition in determining the requirements for technologies to be used in implementing IoT, and checks to make sure infrastructure is ready before the use of IoT is made obligatory. Internet of Things technologies should simplify, not complicate, good business practices and government procedures of law enforcement and inspection.

References

Anthopoulos, L., Janssen, M., & Weerakkody, V. (2016). A unified smart city model (USCM) for smart city conceptualization and benchmarking. *International Journal of Electronic Government Research, 12*(2, SI), 77–93.

Ashton, K. (2015). *How to fly a horse: The secret history of creation, invention, and discovery*. New York, NY: Random House LLC.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*, 2787–2805.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly, 27*(3), 264–271.

Braman, S. (2011). Defining information policy. *Journal of Information Policy, 1*, 1–5.

Brynjolfsson, E., Hitt, L. M., & Kim, H. H. (2011). *Strength in numbers: How does data-driven decision making affect firm performance?* Rochester, NY: Social Science Research Network (SSRN). Retrieved November 30, 2017, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486.

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with China perspective. *IEEE Internet of Things Journal, 1*(4), 349–359.

Coates, J. C. (2015). Cost-benefit analysis of financial regulation: Case studies and implications. *Yale Law Journal, 124*(4), 882–1011.

Cordella, A., & Bonina, C. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. *Government Information Quarterly, 29*(4), 512–520.

Criado, J. I., Sandoval-Almazan, R., & Gil-Garcia, J. R. (2013). Government innovation through social media. *Government Information Quarterly, 30*(4), 319–326.

Dawes, S. (2009). Governance in the digital age: A research and action framework for an uncertain future. *Government Information Quarterly, 26*(2), 257–264.

Dlodlo, N., Foko, T., Mvelase, P., & Mathaba, S. (2012). The state of affairs in internet of things research. *Journal Information Systems Evaluation, 15*(3), 244–258.

European Commission. (2017). *Germany Industrie 4.0. Digital Transformation Monitor*. Retrieved February 28, 2018, from https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf.

Fleisch, E. (2010). What is the internet of things?: An economic perspective. *Economics, Management, and Financial Markets, 5*(2), 125–157.

Fountain, J. E. (2001). *Building the virtual state. Information technology and institutional change*. Washington, DC: Brookings Institution Press.

Gil-Garcia, J. R., & Luna-Reyes, L. F. (2008). A brief introduction to electronic government: Definition, applications and stages. *Revista de Administración Pública RAP 116, 43*(2), 221–241.

Gil-García, R., & Pardo, T. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly, 22*(2), 187–216.

Guillemin, P., & Friess, P. (2009). *Internet of things strategic research roadmap*. The cluster of European research projects. Technical report.

Harlow, K. C., & Windsor, D. (1988). Integration of cost-benefit and financial analysis in project evaluation. *Public Administration Review, 48*(5), 918–928.

Harrison, T. M., Pardo, T. A., & Cook, M. (2012). Creating open government ecosystems: A research and development Agenda. *Future Internet, 4*(4), 900–928.

Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. *The Information Society, 18*, 101–112.

Heeks, R. (2006). *Implementing and managing E-government: An international text*. London: SAGE.

ITU Strategy and Policy Unit. (2005). *ITU internet reports 2005: The internet of things*. Geneva: International Telecommunication Union (ITU).

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly, 32*(3), 221–236.

Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance: Doing more with less. *Government Information Quarterly, 30*(Suppl 1), S1–S8.

Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle: Policy-makers be prepared! *Government Information Quarterly, 35*, S99. https://doi.org/10.1016/j.giq.2015.11.009.

Jin, S., & Cho, C. M. (2015). Is ICT a new essential for national economic growth in an information society? *Government Information Quarterly, 32*(3), 253–260.

Klievink, B., & Janssen, M. (2009). Realizing joined-up government — Dynamic capabilities and stage models for transformation. *Government Information Quarterly, 26*(2), 275–284.

Kraemer, K., & King, J. L. (2006). Information technology and administrative reform: Will e-government be different? *International Journal of Electronic Government Research, 2*(1), 1–20.

Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of things: A systematic review of the business literature from the user and organisational perspectives. *Technological Forecasting and Social Change, 136*, 285–297.

McKinsey. (2015). *Unlocking the potential of the Internet of Things*. Retrieved November 7, 2017, from http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

National Science Foundation. (2017). *Cyber-physical systems (CPS)*. Alexandria, VA: National Science Foundation. Directorate for Computer & Information Science & Engineering. Retrieved November 17, 2017, from https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science, 3*(3), 398–427.

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage.

Potnis, D. (2010). Measuring e-Governance as an innovation in the public sector. *Government Information Quarterly, 27*(1), 41–48.

Radaev, V. (2016). *Main forms of the illegal turnover of the production on the Russian consumer markets and counteraction steps* (Presentation of the Research). Retrieved August 4, 2017, from https://iq.hse.ru/news/199111386.html. (In Russian).

Revesz, R. L. (2017). Cost-benefit analysis and the structure of the administrative state: The case of financial services regulation. *Yale Journal on Regulation, 34*(2), 545–600.

Shevernev, Y. (2016). Means and methods of tagging – The development of the systems tracing industrial products – Technological forms of counteraction to illegal exchange of industrial production in EEU. *International Forum "Anti-Counterfeiting 2016," Yerevan, Armenia, Presentation*. Retrieved from http://nisse.ru/projects/?ELEMENT_ID=132015&sphrase_id=1314106. (In Russian).

Soloviev, N. (2010). Problems involved in the practice of house arrest. *Russian Investigator, 13*. 12p (In Russian).

Statistics Database of the Judicial Department of the Supreme Court of the Russian Federation (2011) http://www.cdep.ru/index.php?id=79 (accessed August 4, 2017).

van Veenstra, A. F., & Kotterink, B. (2017). Data-driven policy making: The policy lab approach. In P. Parycek et al. (Eds.), *Electronic participation. ePart 2017. Lecture notes in computer science* (Vol. 10429). New York, NY: Springer.

van Waart, P., Mulder, I., & de Bont, C. (2016). A participatory approach for envisioning a smart city. *Social Science Computer Review, 34*(6), 708–723.

WEF. (2016). *Digital transformation initiative in collaboration with Accenture*. Retrieved October 27, 2017, from http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/170328-dti-executive-summary-slideshare.pdf.

World Bank. (2016). *World development report 2016: Digital dividends*. Retrieved February 28, 2018, from http://www.worldbank.org/en/publication/wdr2016.

Yin, R. K. (1984). *Case study research: Design and methods*. Newbury Park, CA: Sage.

Zerbe, R. O. (1998). Is cost-benefit analysis legal? Three rules. *Journal of Policy Analysis and Management, 17*(3), 419–456.

Zerbe, R. O. (2004). Should moral sentiments be incorporated into benefit-cost analysis? An example of long-term discounting. *Policy Sciences, 37*(3–4), 305–318.

Zuurmond, A. (2005). Organisational transformation through the internet. *Journal of Public Policy, 25*, 133–148.

Alexander Knutov is a research fellow at the Institute for Public Administration and Governance (IPAG) of the Higher School of Economics National Research University (HSE NRU). Mr. Knutov is an expert in administrative regulation, law enforcement, and inspection issues for Russian government authorities. He also specializes in contract and procurement management, especially research on competition as a method of procurement. Mr. Knutov participates in the review of procurement complaints in the Federal Antimonopoly Service. In the sphere of government inspections of business entities, Mr. Knutov is a member of the group of authors that prepares the annual state report on control and supervisory activities in the Russian Federation. He has done annual research on these issues since 2013 for the Russian Union of Industrialists and Entrepreneurs.

Evgeny Styrin is a leading research analyst and an associate professor affiliated with the National Research University Higher School of Economics. Mr. Styrin provides expertise to Russian public administration bodies. He is an advisor to the Russian Open Government Council. His fields of expertise are public services performance management, open government, electronic government, interagency information sharing, open data, and public IT strategy development and evaluation. Mr. Styrin develops and conducts training courses, teaching students and civil servants in the area of e-government, open data, strategic IT planning, and civil service. As a Russian e-government expert, Dr. Styrin participates in international research projects with the World Bank, UNDP, and OECD.

The Recognition of the New Digital Entrepreneurs in France: The Case of the French Tech with the Emergence of the Internet of Things

Christophe Premat

Abstract Since 2014, the question of the implementation of the Internet of Things has been crucial in France. Public authorities have created arenas where digital entrepreneurs and politicians can discuss the evolution of the Internet of Things. In January 2017, the National Assembly published a report on the economic and social consequences of the adaptation of the Internet of Things. This chapter analyzes the political discourse that gives legitimacy to the implementation of the Internet of Things in France. The digital entrepreneurs are the privileged actors of this implementation; their social recognition by the French Parliament and the labelling campaigns (French Tech) reinforce the myth of technological innovation. The field of the critical analysis of discourse is mobilized to evaluate the spread of this new myth in France and the analysis of the legitimization of the digital entrepreneurs. This case study reveals how European countries tackle new digital policies in order to control the evolution of the Internet of Things and the field of artificial intelligence.

Keywords The Internet of Things (IoT) · Myth · French Tech · Digital entrepreneurs · Protection of innovation · Vocational training · Critical discourse analysis

C. Premat (✉)
Department of Romance Studies and Classics, Stockholm University, Stockholm, Sweden

Centre for vancement of University Teaching, Stockholm University, Stockholm, Sweden
e-mail: chr.premat@su.se

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_8

Abbreviations

ANSES	French National Agency of Sanitary Safety
CDA	Critical Discourse Analysis
DNA	Deoxyribonucleic acid
EAI	Enterprise asset intelligence
Inria	The Institute for Research in Computer Science and Automation
IoT	The Internet of Things
NFC	Near field communication
NGO	Nongovernment organizations
PPP	Public–private partnership
WIPO	World Intellectual Property Organization

Introduction

Many official declarations have enhanced the innovative aspect of the digital economy in France. The creation of new governmental agencies was conceived as an adaptation to the transformation of the world operated by new technologies. The problem is to consider a specific level of legislation that reflects on technologies that do not have any frontiers. The law-making process has been affected by the evolution of digital technologies, and political attitudes seem to swing between an optimism in terms of digital growth and a fear to see processes that threaten national sovereignties in globalization. The IoT is a strong revolution as the communicative process exceeds the single aspect of relations between human beings. This chapter examines how public authorities in France have encouraged digital innovations to boost economic growth. The recognition of new economical actors is fundamental to understanding this process. The genesis of French Tech is an appropriate example of the cultural shift in the political discourse. Digital entrepreneurs are targeted by a new political discourse (Tardieu 2005) that focuses on the innovative impact of the IoT, even though there is a will to simplify administrative hurdles. The main hypothesis here is that there is a new *topos* in the political discourse (Salama 2011: 56) in France, as many politicians emphasize the model of the entrepreneurial self-made man. The National Assembly in France supports the evolution of the digital sector as well as the government that takes initiatives to label the innovations of the digital entrepreneurs. The trust in these new actors can be seen in contrast to the suspicion extended towards politicians; these entrepreneurs receive more and more support from the State, which enrolls experts in new technologies to strengthen a discourse on digital innovation. Digital entrepreneurs activate a disruptive innovation: "What makes such innovations disruptive is that they create new dimensions of value that the old product category or business model is unable to address by satisfying unmet or underserved needs. In other words, they compete based on a different set of benefits that the new approach or technology enables" (Paetz 2014: 6). The IoT deepens

this disruptive model by bringing consumers and companies closer to each other. The companies do not rely only on consumer demand, they can anticipate consumer needs by activating the possibilities offered by the IoT. The analysis of the political discourse helps to understand the prevalence of entrepreneurs in society and in the economy. The parliamentary discussion in France is an appropriate place to analyze the political discourse on digital entrepreneurs. The work of committees is devoted to political confrontation with experts in the field of digital economy. As the parliamentary discussions contribute to a long-term debate, questions of economic innovations are naturally taken into account. The digital law of 2016 highlighted the digital matters in political discussions (Premat 2018).

First, it is necessary to qualify the change of the philosophical paradigm that the IoT provokes. Then, public support for French start-ups will be analyzed in a context of fragile economy and fragmented labor market. The authorities have difficulties to promote a digital growth and create the conditions of tax reforms that would sustain this innovation. With the IoT, there is a threat of getting into a mass surveillance system with a total marketing process that could damage the notions of privacy. The used material includes parliamentary reports on the digital innovation, the governmental agenda on the French Tech label and some public expressions of politicians and digital entrepreneurs.

The critical discourse analysis defended by Norman Fairclough is important to understand the evolution of the discourse on the digital economy with the emergence of the IoT. The discourse here is "interpreted/evaluated/critiqued specifically in terms of contradictions between what it is claimed and expected to be and what it actually is (I shall explain this below); [the discourse] is explained specifically in terms of how such contradictions are caused by and are a part of (sometimes a necessary part of) the wider social reality which they exist within" (Fairclough 2015: 9). The optimistic view of the IoT (growth, innovation, and new services and facilities) is counterbalanced by the perception of societal changes that it can imply. At the same time, the study is all the more interesting as it reveals open and active lobbying from companies and start-ups specialized in digital issues. The social recognition of these actors might be a way of legitimizing an active lobbying form of those companies that promotes lower taxes for business activities in IoT.

The Critical Discourse Analysis

The critical discourse analysis (CDA) is a theoretical paradigm that examines the relation between the social contexts and the production of discourses. The interaction between the sociocultural environment and the scenes of enunciation is all the more important as it enlightens the construction of a doctrine (Foucault 1971). In this context, the CDA reveals the way digital prophecies are embedded in specific social practices. Discourses include the construction of the scene of apparition, what Dominique Maingueneau calls the "scenography" (Maingueneau 1998: 60–64); they reflect the way some words or expressions become common references.

According to the CDA, it is impossible to separate the production of discourses from social identities and roles. “The identities of people who operate in positions in a practice are only specified by the practice itself. People who differ in social class, in gender, in nationality, in ethnic or cultural membership, and in life experience, produce different ‘performances’ of a particular position” (Fairclough 2001: 123). In other words, the CDA focuses on the dialectics between the social positions, the discourses, and the consciousness of the structure of power. The idea is to examine the sociology of actors to understand how they interfere with the current discourse and how they emphasize some utterances. “Social actors involved in discourse do not exclusively make use of their individual experiences and strategies; they mainly rely upon collective frames of perceptions, called social representations” (Meyer 2001: 21). In this chapter, the research topics focuses on the ethnography of the political discourse that gives an added value to digital innovations. The Parliament in France produces reports, hearings, and roundtables on this topic to see how legislation could be adapted to facilitate these innovations.

It is also interesting to point out the implicit interdiscursivity of these debates as the question of digital innovation is dealt with in other political contexts. A debate is not self-sufficient; it uses concepts and sometimes paradigms that justify social practices. Fairclough argues that researchers should produce both academic and nonacademic texts to analyze the construction of some typical discourses that inaugurate a new domain, such as is the case for digital innovation. The CDA and the analysis of public policies could complete each other. In the analysis of public policies, the labels are really important, as they become the key references to the elaboration of new concrete policies (Padioleau 1982). The interaction between digital entrepreneurs and politicians is important, as it concurs to define a set of public policies in the domain of digital innovation. Scholars have defined the role of *référentiel* (Muller 2009: 33), as when politicians and actors involved in a domain negotiate to create a brand that will be used as the reference for an upcoming set of public policies (Jobert 2004: 46). In other words, the *référentiel* could be seen as the result of an active lobbying, where politicians and business partners redefine what should be encouraged by the governmental agencies. In a neoliberal economy, active lobbying is the most efficient way to influence the law-making process towards better rules for the market. In order to reach this level, it is necessary to organize the relations between law-makers and business leaders. The concept of governmentality designed by Michel Foucault (Foucault 2010) is all the more efficient, as it describes a new understanding of power with a new culture (Sennett 2006) that links government to mentalities. The neoliberal governmentality is characterized by a decentered way of governing, where power is not something hierarchical controlled by nation states. It explains why discourses need to be studied, in so far as they reflect a set of norms and values that influence the definition of public policies. The law-making process is challenged by the production of norms and behaviors that do not necessarily suppose the definition of laws.

The Change of Philosophical Paradigm

The IoT is a concept that refers to the connection of things between themselves. It is a strong digital revolution as the flow of information does not need a classical connection between individuals. The things are automatically connected and data are exchanged through the activation of algorithms. The perception is totally inversed. A German philosopher made a difference between things, animals, and human beings. He wrote that an animal was poor in world relations, whereas a human being was full of networks, and a stone had absolutely no possibilities to have relations (Heidegger 1998). From a phenomenological perspective, the things reflect the way human consciousness perceives them. The world means a set of relations between human beings, where values and codes are exchanged to produce a collective meaning. With the IoT, the things have no footprints, they react and give precious information to human beings, and they quit their state of inertia to help people. They contain data and information; this is why they have a digital value (Eldred 2009). The IoT shows the connection of digital objects that have a flow of information that can be used in another context without the human being knowing it. Things are in the world, but they do not exist in the sense of Heidegger. To exist means having connections to the world. "Plants and animals are as well, but for them being is not existence, Dasein, but life. Numbers and geometrical forms are as well, but merely as resource [*Bestände*]. Earth and stone are as well, but merely present [*vorhanden*]. Humans are as well, but we call their being as historical existence, Dasein" (Heidegger 1998: 135; Elden 2006: 276). Things are present in this context in their horizon of utility for human beings that inserts them in a network of available resources. With the IoT, this availability is reversed in the time process, as things can anticipate information and interfere with human actions. "It now becomes clear that we understand the term 'thing' in both a narrower and a broader sense. The *narrower* or limited meaning of 'thing' is that which can be touched, reached, or seen, i.e., what is present-at-hand (*das Vorhandene*). In the *wider* meaning of the term, the 'thing' is every affair or transaction, something that is in this or that condition, the things that happen in the world—occurrences, events" (Heidegger 1968: 5). The IoT allows a connection between inanimate objects; the sensors capture data and send back information, and the interoperability of objects is important. Inanimate objects have two categories of objects: fixed objects such as buildings, industrial plants, machines, fixed assets, posters, and moveable objects such as transport, vehicles, large containers, transport units, devices, mobiles phones, smartphones, iPads. Animate things include persons, animals, anatomic parts, cells, and DNA (Chaouchi 2010: 8). Sensors create the possibilities for ubiquitous computing; they increase the speed of connection between objects.

The IoT includes communication at any time (indoors, outdoors), and the interaction can be from person to person, machine to machine, machine to person. The classical digital communication modes, such as near field communication (NFC) (Coskun et al. 2011), are also used by the IoT. "NFC is a technology that simplifies and secures the interaction with the automation ubiquitously around us. The NFC

concept is designed from the synergy of several technologies including wireless communications, mobile devices, mobile applications and smart cards" (Coskun et al. 2011: 2). With the NFC, we are still in a model of human–human communication based on a wireless data transfer. It is better to combine former theories to understand the change of the world that the IoT implies. For his part, James Gibson has developed a theory of affordance on the ecological approach to the environment (Gibson 1986). There are sensors present in the environment that are integrated in a larger system of communication. Objects already have a cognitive potential, because they receive semantic instructions; there is then a continuity between the mind and the world (Paveau 2012: 55). With the sensors, the things conserve information that can be reused. Transhumanist theories promote the idea that human beings are transformed with the help of biotechnologies. The IoT has a major impact on health, the connected things bring more knowledge that can be used to improve human life. From transhumanist perspectives, there is the belief that the science can solve all problems and that human beings can advance to "higher levels of existence and experience" (Hauskeller 2016: 8). As a matter of fact, it is easier to analyze the public agenda (Dearing and Everett 1996), and the way digital entrepreneurs and politicians have built a public discourse on digital economy from these different views of the impact of connected objects and sensors.

The International Context for the Digital Agenda and the IoT

President Obama talked about an open Internet that should be promoted in globalization in his State of the Union's address in January 2016. "In fact, it turns out many of our best corporate citizens are also our most creative. And this brings me to the second big question we as a country have to answer: how do we reignite that spirit of innovation to meet our biggest challenges? […] America is every immigrant and entrepreneur from Boston to Austin to Silicon Valley racing to shape a better future. That's who we are, and over the past seven years, we've nurtured that spirit. We've protected an open Internet, and taken bold new steps to get more students and low-income Americans online."[1] The national narrative is in this perspective reinforced with the core idea that Americans constitute a nation of entrepreneurs. The connection of immigrant to entrepreneur is a part of the American dream, and Silicon Valley is a current incarnation of that pattern. The Obama administration facilitated investments in the digital economy. Business, governments, and consumers are affected by these innovations.[2] The American Senate proposed a bill on the Internet of Things to preserve business concerns, and protect innovations while

[1] https://www.nytimes.com/2016/01/13/us/politics/obama-2016-sotu-transcript.html Retrieved 19 February 2018.

[2] http://www.businessinsider.com/obama-administration-helps-smart-city-growth-for-iot-internet-of-things-2016-3?r=US&IR=T&IR=T Retrieved 19 February 2018.

granting better security of data.[3] Last but not least, the House of Representatives held a debate on these issues in the subcommittee for digital commerce and consumer protection.[4] The question of IoT is still sensitive for US authorities, as the country wants to maintain a high degree of digital innovation, which is compatible with the fight against cyberattacks.[5]

Many governments are interested in digital innovations, as they see potential effects on growth and jobs. In these political discourses, it is possible to see that many firms become political actors by influencing norms and the political debate. The digital innovations are a part of the New Public Management system, where the private sector transfers norms of governance and patterns to the public sector (Pollitt and Bouckaert 2004: 155). The firms define rules and norms that are reused in the political system. This is why the open internet can be seen as a transfer of power to transnational firms that control the innovations in IoT. The public–private partnership (PPP) is often the methodology used by governments trying to deal with digital innovations. The international context reveals, in fact, that transnational firms play a political role (March 1962), by putting pressure on different political systems to implement public policies on digital matters that they will then execute (Barley 2007: 202).

The conclusion of the statement of Rodney Masney, Vice-president of Technology Service Delivery of the Information Technology Owens-Illinois Corporation, is worth comment, as he addressed a few recommendations to the public authorities concerning IoT issues. He proposed that the public authorities could (1) Assist manufacturers in making IoT technologies more affordable by encouraging research and investment in these capabilities or in programs which encourage manufacturing companies to deploy IoT solutions, (2) Support programs or resources that address cybersecurity in US businesses, (3) Encourage more research in the IoT data science discipline and seek ways to encourage a supporting pipeline of skilled workers through universities and manufacturing related technical tools."[6] Such investments assume facilities and lower taxes for the business environment, adapted programs at universities that target engineers, and people that can conduct these projects. Technology, capabilities, and data are key words for people working in the field of IoT. Tom Bianculli, chief technology officer at Zebra Technologies, has summarized in an interview the basic needs in this field of innovation. He has presented a

[3] https://www.reuters.com/article/us-usa-cyber-congress/u-s-senators-to-introduce-bill-to-secure-internet-of-things-idUSKBN1AH474 Retrieved 19 February 2018.

[4] https://energycommerce.house.gov/hearings/disrupter-series-internet-things-manufacturing-innovation/ Retrieved 19 February 2018.

[5] Congressman Pallone (New Jersey) put emphasis on that balance in his statement during the hearing. https://energycommerce.house.gov/hearings/disrupter-series-internet-things-manufacturing-innovation/ Retrieved 19 February 2018, "As with all connected technologies, strong cybersecurity is essential to successful smart manufacturing" (https://democrats-energycommerce.house.gov/newsroom/press-releases/pallone-opening-remarks-at-internet-of-things-hearing)

[6] http://docs.house.gov/meetings/IF/IF17/20180118/106781/HHRG-115-IF17-Wstate-MasneyR-20180118.pdf Retrieved 20 February 2018

new business model in the following terms: "The organisation is moving from what we call enterprise mobility to a new category called Enterprise Asset Intelligence (EAI). At the heart of EAI is IoT. There are three main pillars to EAI—Sense, Analyse, and Act. The notion behind Sense is to sense data at the edge of our customer's networks, gather that data, and aggregate that in the cloud. Then we analyze data."[7] Most of the companies working within IoT capture data and use them to create a system of information that facilitates customer needs.

If different national Parliaments organize talks and events in the field of IoT, it is interesting to see that the domain of the IoT in the USA is associated with big corporations, whereas, in other countries, the IoT is perceived as an innovative sector trusted by start-up companies. This was demonstrated in the UK with a discussion that was held in the House of Commons on 24 October 2018.[8] The speech given by Rachel Cooper, OBE from Lancaster University, reveals the common discourse on the IoT: "It is clear that the UK is leading in terms of the number of start-ups in digital technology, IoT and related technology. Indeed, we have more start-ups in machine learning than anywhere else in Europe. The attendees noted that this is an important growth area for the UK and we need to consider how we help these companies scale up, what sort of investment packages could ensure they scale up in the UK."[9] The scale argument is important in Europe, as many start-ups have invested in the sector of the IoT in contrast to start-ups in the USA, where big corporations manufacture these technologies. This contrast may explain why the public authorities try to support the efforts made by start-ups to reach a sustainable and competitive model in the domain of the IoT. The case of France is interesting as the IoT was considered as a potential sector for innovation inside the digital economy. In a context of weak growth, there is a tendency in the French political discourse to capture this innovation by empowering the key actors that work on the IoT.

The Public Support for French Start-Ups

To analyze the political discourse in France on the IoT and digital innovations, it is necessary to study some key information reports, such as parliamentary reports, where the political consequences of digital innovations are presented as well as actions of the government and discussions with digital entrepreneurs. The CDA helps to identify the interactive discussion (De Chanay and Turbide 2011) between politicians and corporations on digital matters, as well as the typical rhetorical patterns that are used and produced in this discussion (Fairclough 2001: 128).

[7] http://www.sramanamitra.com/2016/06/27/thought-leaders-in-internet-of-things-tom-bianculli-vice-president-of-technology-office-at-zebra-technologies-part-1/ Retrieved first of March 2018

[8] http://www.ipt.org.uk/Events/Event-News/Details/The-Internet-of-Things-and-the-Evolution-of-Smart-Technologies Retrieved second of March 2018

[9] http://www.ipt.org.uk/Events/Event-News/Details/The-Internet-of-Things-and-the-Evolution-of-Smart-Technologies Retrieved second of March 2018

The French government has defined a digital agenda by labelling different French Tech zones between 2013 and 2016. The goal was to stimulate digital innovation by encouraging the activities of French start-ups. France defined this strategy in 2013 in order to be a digital nation that invested in digital growth. The State Secretary on digital economy at that time, Fleur Pellerin, initiated the project of French Tech by announcing the "Start-up Republic" in November 2013.[10] President Hollande inaugurated the French Hub in the Silicon Valley on 12 February 2014 to promote this initiative.[11] The French government contributed 2 million euros per year, but this support was criticized as French Tech was not seen as a diversified structure that could lead to strong innovation. The public authorities felt that they had to adopt the lexicon of globalization/adaptation/innovation by multiplying events, labels, and official declarations on the digital economy. The political discourse is still prophetical in France as the concerned actors are mainly a set of successful start-ups.

The lack of local partners and the weak knowledge of the market environment were pointed out by the critics of this initiative. In this hub, many start-ups were in contact with each other to improve services and increase their productivity. The last time a French president visited Silicon Valley dated back to 30 years ago. The objective of the French hub was to help around 60 French start-ups to work in California.[12] For instance, a French start-up such as talentoday[13] was specialized in professional orientation, whereas Wimi[14] aimed at facilitating work management. The principle of the French hub was to connect French digital start-ups, business schools, and universities with the help of the French government to create strong innovation potential. Table 1 shows the different steps in the labelling of French Tech in France. The top-down process is obvious in Table 1, as the French government highlighted the economic initiatives that could have an impact on growth by gathering researchers and entrepreneurs.

In the French finance law of 2013, 0.6% of investments concerned the field of the digital economy.[15] The question of a relevant business model for this type of economy was dealt with in the finance laws of 2014 and 2015, and the French Parliament began to be active in the field of digital modernization. The French government of Manuel Valls initiated in 2014 a strong business campaign in which the objective was to affirm the potentials of French start-ups in globalization.[16] Officially, France adapted its legislation to the context of globalization pretty much inspired by the

[10] It is interesting to point out that Emmanuel Macron devoted a part of his presidential campaign in 2017 to that topic.

[11] http://lexpansion.lexpress.fr/high-tech/hollande-inaugure-le-french-tech-hub-de-san-francisco-sur-fond-de-polemiques_1333899.html, 12 February 2014, retrieved 17 May 2017.

[12] http://www.20minutes.fr/high-tech/1297666-20140213-20140213-francois-hollande-inaugure-french-tech-hub-coeur-silicon-valley, 13 February 2014. Retrieved 17 May 2017.

[13] https://www.talentoday.com. Retrieved 17 May 2017.

[14] https://www.wimi-teamwork.com. Retrieved 17 May 2017.

[15] http://www.assemblee-nationale.fr/14/pdf/projets/pl1395.pdf. Retrieved 19 May 2017.

[16] http://www.gouvernement.fr/en/manuel-valls-in-davos-france-is-here-to-say-that-it-is-implementing-strong-and-courageous-reforms. Retrieved 19 May 2017.

Table 1 Different steps in labelling French Tech

Date	Political announcements/acts
November 2013	The label French Tech is initiated for French start-ups
January 2014	Call for applications for French Tech metropoles
Between January and November 2014	Creation of a mission French Tech that evaluates applications by visiting all sites.
12 November 2014	First wave of labels with 9 French Tech zones
25 June 2015	Second wave of labelling
19 January 2016	Call for applications for thematic networks French Tech
29 January 2016	Evaluation of the first wave of labelling
4 April 2016	End of the call for applications for thematic "French Tech"
June 2016	Evaluation of the second wave of labelling
25 July 2016	Announcement of the constitution of thematic networks and renewal of labelling

Source: French Tech

ideas of restructuring the labor market. If there is no support from public authorities in France, the future of the IoT might be outside the country; this is why the government is concerned about these innovations. The political discourse on the risk of delocalization is still active to avoid the loss of wealth. This is why politicians are compelled to have a pro-business attitude in order to attract investments in and companies to France. As a matter of fact, they contribute to the conception of the "doctrine" (Foucault 1971: 45), which means the common discourse that many people have. The doctrine consecrates the importance of the discourse that circulates among many actors. The French government focuses on the digital prophecy by reusing and recycling a common discourse that prevails in many countries.

In 2014, Corinne Erhel and Laure de La Raudière presented a parliamentary work on digital economy to the Committee of Economic Affairs of the National Assembly. This parliamentary report is important as it characterizes French contributions to the digital economy. In 2014, 60,000 French entrepreneurs and engineers were located in Silicon Valley and some French successful start-ups were mentioned in the report. Table 2 shows a list of the successful start-ups that have a strong international reputation. These start-ups could find a sustainable model by creating a sales platform with a modest number of employees. *Dailymotion,* which is a francophone version of *YouTube,* has just 180 employees as the value is produced by consumers who use the possibilities of the platform.

In their report, Corinne Erhel and Laure de La Raudière highlighted the development of e-business, the use of e-currencies, such as bitcoin (Gimigliano 2016) launched in 2009, and the emergence of connected objects in the field of health. The company Withings, for instance, is specialized in the connection of different objects related to health. The company developed connected objects to follow up patients and was bought by Nokia at the end of 2016. The different reports submitted to the French Parliament illustrate the necessity to secure the digital economy. Table 3

Table 2 Successful French start-ups

Name of the start-up	Year of creation	Number of employees (2017)
Parrot	1994	948 employees in 2015
Priceminister	2000	Around 250
Exalead	2000	150
Doctissimo	2000	45
Meetic	2001	300
Vente-privee.com	2001	Around 2000
Criteo	2005	1750
Dailymotion	2005	180
Deezer	2007	300 or 400

Source: own research on the official numbers declared by the different companies

sums up all the parliamentary reports on this question between 2012 and 2017. The French Parliament is composed of two chambers, and below is a list of the reports published by the Senate and the National Assembly.

Twelve parliamentary reports on digital affairs were published between 2012 and 2017, and a law on the Digital Republic was adopted, the goal of which was to strengthen digital practices and make France a digital nation. The IoT was dealt with in these reports, especially in Report Number 4362 by Corinne Erhel and Laure de La Raudière (2017), which was exclusively devoted to this question. The report by those authors insists that governmental efforts join with French Tech to promote the field of digital economy. Thanks to tax exemption policies, the innovations were secured through different budgetary discussions in 2014, 2015, 2016, and 2017. French Tech was conceived as a new opportunity to promote the creation of French start-ups in different local ecosystems.

In July 2016, 13 French Tech labels were given to French municipalities that work with digital innovations. The business model was built with the cooperation between different types of technologies with the support of local governments. This is really important to maintain high-quality technology in France and avoid a loss in growth. The example of IoT Valley in Toulouse is worth commenting. Toulouse holds a leading position in the field of aviation. It was created in 2009 by four entrepreneurs from Toulouse.[17] The association of companies and start-ups (more than 40) helped to create an accelerator program, LeConnected.Camp,[18] which is mostly financed by private funds and has partnerships with major groups like Microsoft and Samsung. A digital campus was built on the site of Labège-innopole to increase links between start-ups.

The National Assembly took part in the promotion of digital economy. A round-table on digital innovation was held at the National Assembly on 30 September 2015 thanks to the Committee of Economic Affairs. Some digital entrepreneurs were invited to discuss and present the main challenges of digital innovation. One

[17] http://www.iot-valley.fr/eng#accelerator. Retrieved 20 May 2017.

[18] http://leconnected.camp. Retrieved 20 May 2017.

Table 3 Parliamentary reports on digital topics between 2012 and 2017

Parliamentary report on digital matters	Official date	Registered number	Topic
Alain Calmette	14 November 2012	No. 398 (National Assembly)	Digital territory of the development
Axelle Lemaire/ Hervé Gaymard	8 October 2013	No. 1409 (National Assembly)	Digital strategy of the European Union
Corinne Erhel/Laure de La Raudière	14 May 2014	No. 1936 (National Assembly)	Development of the French digital economy
Christian Paul/ Christiane Féral-Schuhl	8 October 2015	No. 3119 (National Assembly)	Digital world and liberties: a new democratic age
Hervé Maurey/ Patrick chaize	25 November 2015	No. 193 (senate)	Digital connection of territories: to control the respect of the engagements to avoid new disillusions
Luc Belot	15 January 2016	No. 3399 (National Assembly)	Law report on Digital Republic
Christophe-André Frassa	6 April 2016	No. 534 (senate)	Law report on Digital Republic
Luc Belot/ Christophe-André Frassa	30 June 2016	No. 743 (senate/ National Assembly)	Bill for Digital Republic (mixed committee)
Michel Canevet	26 October 2016	No. 76 (senate)	Public information: which possibilities for the administration?
Corinne Erhel/Laure de La Raudière	10 January 2017	No. 4362 (National Assembly)	The IoT
Marietta Karamanli	7 February 2017	No. 4527 (National Assembly)	The digital single market and the initiatives for regulating the platforms
Jacques Mézard/ Philippe Mouiller	19 April 2017	No. 509 (senate)	New technologies for the modernization of territories

Source: own research

of the entrepreneurs, Ludovic Le Moan, told the members of the committee the success story of his start-up. "In 2011, in Toulouse, we were two. Today we are just over 150, and we are present on the East Coast of the USA, Dubai, Singapore, and various European countries. We are in the process of deploying a network that will connect everything in the physical world to the virtual world."[19] According to Le Moan's discourse, the international success of the company will be enhanced if new territories are discovered, thanks to the IoT. A start-up becomes a globalized corpo-

[19] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 13 July 2017). The translation into English is ours.

ration with strong connections. In this discourse, the start-up entrepreneur is a pioneer who seeks a model for aggregating and analyzing data to facilitate a specific need. Le Moan has stated that he regretted that investment possibilities were limited in France[20]. In the observations made by French digital entrepreneurs during this hearing, there is always the mention of the American example. The USA is presented as a strong market with many facilities that has financial support, whereas the European legislation is complex, and the national markets are too limited. The American dream (the perception of size, the abolition of limits, openness) prevails in the discourse of digital entrepreneurs in France.

Montpellier French Tech has had the same synergy of start-ups since 2015. The local authorities would like to improve this business model otherwise they fear an exit solution (Sethi 2016: 189–196); a lot of start-ups prefer to secure their existence by joining a major group such as Google or Apple. For instance, in the meeting held by the Committee of Economic Affairs of the National Assembly, a digital entrepreneur mentioned how the acquisition of a part of a start-up could be the best option in terms of financial stability. Cécile Lazorthes, founder of *Leetchi*, presented to the committee the story of her start-up which is specialized in birthday gifts[21]. As far as she is concerned, the financial stability is the most important thing for innovative start-ups, especially in a fragmented and competitive market. Many digital entrepreneurs regret that there is no single market in the European Union, and they have to devote time to follow the different legislations of the countries in which they are represented. This is an important point in discussions at the national level, many politicians and digital entrepreneurs claim that substantial changes could be enshrined in European legislation (Weber and Weber 2010: 71).

Éric Carreel, president and founder of *Withings*, said to the members of the Committee that it was easier to be an entrepreneur in France nowadays than 20 years earlier[22]. This is an evolution of the labor market that makes these digital start-ups create self-regulation of employees. It is now possible to "replace hierarchical management with self-governing teams, the rising influence of managers and coaches vis-à-vis directors and executives from command and control to self-managing groups and quality circles, from control to self-control" (Triantafillou 2012: 115). If digital entrepreneurs specialized in the IoT want to have fewer administrative tasks and fewer constraints, they are also conscious of the opportunities of these connections, which allow many companies to develop individual services. If people and things are connected, there are resources to develop a new disintermediation to avoid complications. This a new step in the self-entrepreneurial culture (Corbett and Katz 2013: XII), where many new companies can emerge thanks to a positive business environment.

---

[20] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp. The translation into English is ours. Retrieved 25 May 2017.

[21] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 13 July 2017). The translation into English is ours.

[22] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 13 July 2017). The translation into English is ours.

In Montpellier, the start-up "Big up for start-up" is a company created in the French Tech of Montpellier and that creates a network of opportunities for digital businesses. They accelerate the possibilities of services by organizing events that are supposed to create new digital projects. The report by Erhel/de La Raudière underlines the engagement of public authorities in the sector of the IoT, but deplores a lack of international investors due to a complex environment in terms of labor organization and taxes. The reform of taxes for wealthy persons is mentioned by those authors as the business model of all those start-ups can benefit from international investments. The tax question is addressed in the context in which transnational corporations developed lobbying activities to lower taxes (Nownes 2006: 59). The economic model for start-ups is composed of crowdfunding possibilities, and co-financing thanks to the investment of a major group. This economic model has difficulties translating into tax legislation, according to Erhel/de La Raudière. In the modified financial law of 2016, an amendment was introduced to facilitate the development of the small- and medium-sized enterprises (Passerini et al. 2012: 3).[23] This was an important step to facilitate the implementation of an adapted economic environment for start-ups. The creation of this account encourages persons involved in the management of their business (entrepreneurs, founders, managers, and employees holding capital) to reinvest their capital gains in new companies to which they will also bring their professional network.

The Committee of Economic Affairs of the National Assembly held hearings with some well-known digital entrepreneurs to see how this business model could be reinforced in France. On 30 September 2015, a roundtable was organized at the Assembly on the topic of the digital economy with Éric Carreel, founder and president of *Withings*, Céline Lazorthes, founder and president of *Leetchi*, Frédéric Mazzella, founder and president of *Blablacar*, Ludovic Le Moan, founder and president of *Sigfox,* and Simon Baldeyrou, CEO of *Deezer France*. In his presentation, Frédéric Mazzella emphasized the young profile of the members.[24] The IoT is a new trend that requires young entrepreneurs that can adapt to the evolution of these technologies; professional experience does not have the same value as in the past, because the attitude towards new technologies is preferred. It costs less for a company to train young entrepreneurs that can adapt and sometimes create their own tasks with the aim of reinforcing the competitiveness of the company. In this perspective, uncertainty and flexibility are the main components of the new corporate culture (Sennett 2006: 16).

[23] http://www.assemblee-nationale.fr/14/amendements/4235/AN/221.asp (Retrieved 15 July 2017).

[24] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 15 July 2017). The translation into English is ours.

Belief in Digital Growth and the Capture of Expertise

In France, the official discourse always presents the digital transition as a source of innovation. Without defining rigorously what the digital era means, there has been a flow of statements about the necessity of investing in digital challenges (Thibault and Mabi 2015: 162). The idea is to produce tools similar to those in the USA with the development of a strong French Tech. The search for labels is constant as digital design is perceived as the main characteristic of an innovative country. An analysis of the video of the roundtable of the meeting of the Committee of Economic Affairs shows strong connivance in the interaction between the MPs and the digital entrepreneurs. Indeed, the president of the committee had selected and invited those entrepreneurs who were perceived as representative of the field. All the reactions of the MPs show that they share this interest in a new model of digital economy, which is seen as a step forward in the innovation and creation of new jobs.

The discourse of the participants of this roundtable is worth commenting on. In this example, the differentiation between *langue* and *parole* is used to analyze the political discussion on digital evolutions. The concept of *parole* refers to the language used in specific social contexts (Fairclough 2015: 54). For instance, Corinne Erhel, a socialist MP, who is one of the few MPs specialized in the digital sector, began her questioning at the roundtable by congratulating the different digital entrepreneurs. These introductory words are far from being just a mark of politeness. "You are a generation of bold entrepreneurs. You have helped to shake up your industries and habits by shaking up old models and creating new ones. I agree with you when you say that we probably missed the challenges of digital innovation.[25] The words "bold entrepreneurs" ("*entrepreneurs plein d'audace*") mark the social recognition of digital entrepreneurs, who take risks in a complex business environment. All the MPs asked questions about how to improve the possibilities of these sectors. For instance, the other MP from the Conservative Party, Laure de La Raudière, who is also an expert in digital issues and who was present at the roundtable, dealt with the necessity of having a cultural shift in France. "You mentioned the need for a change in culture, which is even more complicated. Because there is a real border between your trades, your generation, and the traditional world. One of you said that the administration should be valued by the initiatives it is taking. […]. In any case, it is a change of culture to ask the administration to take risks."[26] This statement illustrates the social identities of the actors, who are curious and enthusiastic about the economic impact of such a sector. In this context, digital entrepreneurs emphasize flexibility and a culture of risks. A discourse analysis of this roundtable illustrates the fact that, in terms of address, the committee has already designed the ideal type of the modern digital entrepreneur. The appetite for

[25] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 15 July 2017). The translation into English is ours.

[26] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 15 July 2017). The translation into English is ours.

newness was obvious, and the differentiation between the traditional attitudes and the new world were amplified during the presidential campaign of Emmanuel Macron. "Language is a part of society; linguistic phenomena *are* social phenomena of a special sort, and social phenomena *are* (in part) linguistic phenomena" (Fairclough 2015: 56). In the meeting held by the Committee of Economic Affairs, the speakers, who know that they are being recorded, share the same positive attitude towards this field that is quite mysterious for them. All the participants related themselves to the technological myth of the IoT. They tried to anticipate the consequences of such transformations. According to Neil Gillman, "myths of this kind can neither be verified nor falsified. They can only be challenged by an alternative myth, and they can be testified against" (Gillman 2004: 95). The discourse on digital economy becomes a myth thanks to the political integration of these aspects, and thanks to the new alliance between public authorities and digital entrepreneurs.

There was a "mutual recognition" (Pinkard 2012: 23) expressed by one of the digital entrepreneurs during the roundtable. The digital entrepreneurs were there to convince the MPs to put more efforts into reforming the administration. Éric Carreel, cofounder of Withings, adopted a very direct style that was noticed during the meeting. The differentiation of roles was affirmed (we create value and jobs and you, the politicians, should facilitate our jobs and reform the administration), each actor had to focus on his/her tasks. "For the administration, I do not have the answer. It is up to you to give it, but the administration needs to be encouraged when it takes initiatives, not when it applies the precautionary principle which seems to me to be a fundamental aberration in this country."[27] The digital entrepreneur gives with these words his feeling on the role of the administration, he would like it to be more creative and risk-taking, and the expression "fundamental aberration in this country" reveals a political opinion. According to Éric Carreel, the cultural shift implies a culture of initiative from the administration. The message was clear and was welcomed by the MPs who took part in the hearing. Éric Carreel described his view on the business world: career changes, flexibility, risks were the keywords of his presentation.[28] Not only did he emit a strong political opinion, but his statement shows that, with the IoT, a new horizon has been reached. The connected objects can increase the immediacy of consumerist reflexes. The idea is to maximize the relation of consumers to new services. "The *commodity* has expanded from being a tangible 'good' to include all sorts of intangibles: educational courses, holidays, health insurance, and funerals are now bought and sold on the open market in 'packages,' rather like soap powders. And an even greater focus has been placed upon the consumption of commodities, a tendency summed up in the term *consumerism*" (Fairclough 2015: 66). The political attention that the digital sphere has attracted in France reveals that there is a new ideological trend that affects the organization of

[27] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 15 July 2017). The translation into English is ours.

[28] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 15 July 2017). The translation into English is ours.

companies. The typical discourse on digital innovation began under President Sarkozy with the creation of a National Council for Digital Affairs.

In 2011, the National Council for Digital Affairs was created as an independent structure that was to focus on the impact of the digital revolution on French society. Former French President Nicolas Sarkozy referred to the necessity of creating such a structure in his speech delivered on 27 April 2011.[29] The speech included many adjectives that enhanced the necessity of structuring the digital sector: "new," "wonderful," "unavoidable." The topics covered in the speech were digital economy, regulation, digital tax reforms, and the struggle against terror threats. In the speech, Sarkozy said this about the new Council: "It is a French initiative, but naturally what we want for the French digital economy would not make sense if what was decided between us was not destined one day to apply to the United States, the United Kingdom, Germany, Japan, and elsewhere."[30] Following this, President Sarkozy described the creation of a structure that could be duplicated in other countries, the structure would reflect on digital innovation but also on the added value produced by the digital economy. The idea was to legitimize the field of digital economy and mix digital entrepreneurs with politicians and senior state officials (Fairclough 2015: 78). The difficulties of law-making were also mentioned in the speech. All the following speeches surrounding the evolution of digital affairs did not really see the paradigm shift between the World Wide Web 2.0 and the IoT.

The National Council for Digital Affairs promoted many ideas that were incorporated in the law on the Digital Republic, which was adopted in late 2016. Net neutrality, loyalty of digital platforms, protection of independent workers in the field of the digital economy, and European digital strategy were seen as the priorities needed to accelerate the digital agenda. *FranceStratégie*, an expertise cell under the responsibility of the prime minister, published a series of recommendations on 8 January 2015[31]. In 2015, according to this report, there were around 15 billion connected objects in the world, and they could be between 50 and 80 billion in 2020. All the efforts of the government aim at regulating this new field as the IoT is a promise of progress (Koerten and Veenswijk 2013).

The Challenge of Vocational Training and the Protection of Innovation

The official discourse on the digital economy perceives the IoT as the last evolution that entrepreneurs must capture to enhance French innovation. The emergence of the IoT is perceived as a communicative revolution. The connections between things

[29] http://discours.vie-publique.fr/notices/117001029.html

[30] It is our translation from French into English. Retrieved 19 July 2017.

[31] http://www.vie-publique.fr/actualite/alaune/internet-objets-quoi-s-agit-il-20150119.html « Internet des objets: de quoi s'agit-il? », 8 January 2015. Retrieved 20 July 2017.

and human needs activate a chain of information that forms without the individuals being conscious of it. The problem is that government authorities present the economic potential of the IoT before describing the anthropological consequences of the speed of connections. The official discourse on the IoT in France shows that digital start-ups, are promoted as the future actors of wealth; corporations are supposed to take care of these common goods. This is a major problem in France when government authorities aim at facilitating business without anticipating the consequences of the IoT (Reich 2007). One of the consequences is the difficulty to associate innovation and employment. With connected objects, it is easy to multiply the chain of new actors proposing new services thanks to all the possible connections that do not need high-speed broadband (Borman 2011: 21). The relation between the IoT and the creation of jobs is not obvious as many traditional activities disappear. The new jobs do not necessarily compensate the disappearance of former ones. In the roundtable of the Committee of Economic Affairs, one of the digital entrepreneurs used the example of Uber to describe the possibilities of new jobs.[32] The potentiality of the IoT depends on the extraction of knowledge from different sensors that can be converted into new services. The digital entrepreneur believes in this form of hybrid connection (Ortolani 2014: 161) with all the smart objects.

During the roundtable, the digital entrepreneurs have insisted on the issue of vocational training to implement long-term policies in the field of the digital innovation. The necessity for specific training is recurrent in the political discourse in France, but the content of such training is quite vague. On this aspect, the cofounder of Withings said that he was worried about the split between highly educated workers and others who had not been trained in recent years. "In digital companies, we have solutions for engineers and for well-trained people. But I am personally very worried about people who have very little training. What can be done for young people who have not worked for five years because they do not have training that can be used in this new environment?"[33] In their report on the IoT, Corinne Erhel and Laure de La Raudière suggested increasing the number of specialized masters in big data such as the master program of *Télécom Paris Tech*.[34] The Institute for Research in Computer Science and Automation (INRIA), created in 1967, initiated in 2011 the technological platform FIT (Future IoT), which combines experiments in robots and radio frequencies. Thanks to this knowledge, three successful start-ups were created: *Alerion* (2015) with smart solutions for drones; *NeoSensys* (2014), which proposes a smart system of image captures for video surveillance; and *Therapixel* (2013), which proposes to surgeons interactive solutions to analyze medical images in operating rooms.

[32] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 15 July 2017). The translation into English is ours.

[33] http://www.assemblee-nationale.fr/14/cr-eco/14-15/c1415079.asp (Retrieved 15 July 2017). The translation into English is ours.

[34] http://www.assemblee-nationale.fr/14/rap-info/i4362.asp#P1020_291709 (Retrieved 20 July 2017).

This innovation requires a form of ongoing training, but at the same time, it must be protected in order to structure the field. Patents must be secured. According to the World Intellectual Property Organization (WIPO), France is the sixth country in terms of industrial patents.[35] The stability of the sector also depends on the ability to hire well-trained employees that can contribute to creating more industrial patents. As stated in the WIPO report: "Patent rights generally last up to 20 years from the date the application was filed. The estimated number of patents in force worldwide rose from 7.2 million in 2008 to 10.6 million in 2015."[36] There can be a legal battle between big companies on the issue of patents, such as between Apple and Samsung, which resulted in banning the Samsung Galaxy Tab tablet from the German market.[37] There can also be debates on the potential damages that certain connected objects can have. In France, there was a debate on the use of smart electricity meters *Linky* with the Act of 17 August 2015 on energy transition for green growth. These smart meters allow for the transmission of knowledge to energy suppliers. In early 2017, the national agency of sanitary safety (ANSES) published a report concluding that *Linky* smart meters could cause health problems.[38] The agency was consulted in 2015 and concluded that *Linky* smart meters could help reduce energy costs and that the damages on health were not proved. This fact shows how uncertain governmental agencies and politicians are in terms of social consequences of some digital innovations.

Broadly speaking, there is a risk of dispossessing individuals of their competencies, as all these connected objects transfer knowledge to facilitate human needs and anticipate potential defaults without people knowing about them. In many fields where human beings have had technological expertise, they could lose a privileged status, as there is no longer any need for the competencies. Dubey and Moricot deal with the idea that the human–machine relation lacks technical competencies. For instance, the pilot of an aircraft no longer has a specific function as the major part of his/her competencies is activated through a connection of objects. The environment is full of smart objects that exclude the technical knowledge that was required earlier (Dubey and Moricot 2016). In their report on the IoT, Corinne Erhel and Laure de La Raudière have concluded that there is a risk of social rupture between those who understand the use of the IoT, and others who will not be able to use the potentiality of the connected objects. This is why vocational training must include both digital workers and users.

[35] http://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2016.pdf (Retrieved 20 July 2017)

[36] http://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2016.pdf (Retrieved 20 July 2017)

[37] http://www.assemblee-nationale.fr/14/rap-info/i4362.asp#P1020_291709 (Retrieved 20 July 2017)

[38] https://www.anses.fr/en/system/files/AP2015SA0210Ra.pdf (Retrieved 20 July 2017)

Conclusion

The French digital agenda shows that the government pays attention to the new field of the IoT. Parliamentary reports and experts on this matter reveal an optimistic discourse on the potentialities of digital technologies. This discourse was made possible with the mutual recognition of digital entrepreneurs and politicians. Digital growth became a myth in the sense that connected objects would substantially modify the perceptions of the world. The French government created the initiative "French Tech" to label projects that can make France a competitive digital nation. These initiatives reflect a storytelling process (Brown 2004), where politicians and digital entrepreneurs show a renewed image of the country. The parliamentary work conducted at the National Assembly, with hearings and reports, shows this interest in digital economy with the most recent innovations. More and more start-ups are becoming visible and corporate culture is beginning to be understood by the politicians who share the same discourse on the necessity of sustaining digital growth. If politicians are aware of adapting legislation in order to support small and medium sized enterprises and start-ups, the required tax reforms are difficult to implement as they would require a change of European legislation. The claim for flexibility is one of the characteristics of this new discourse, it illustrates what the sociologist Zygmunt Bauman defines as "modern liquidity" (Bauman 2005) with the predominance of job mobility, and the idea of destructive creation. The parliamentary reports and the meetings held by the National Assembly reveal a deep consciousness of how to stimulate this innovation in a fragmented labor market. The necessity of training people who understand the consequences of these innovations is dominant. Digital entrepreneurs have succeeded in receiving strong recognition from politicians, but the belief in digital growth does not make difficulties disappear. It is doubtful that the digital sector can reindustrialize the country when time and cost savings are obtained with the use of these technologies. It seems that we have a constructive alignment of ideologies between digital entrepreneurs and politicians regarding the IoT in France, this alliance is due to the belief in the discovery of a new source of wealth. The analysis of the public agenda shows that there is an official discourse on the promise of the IoT with some measures regarding tax reforms and digital education, but the voluntary discourse should give way to a democratic debate on the consequences of the use of connected objects. The main discourse on data economy cannot elude the impact of disruptions (Stiegler 2013); it is necessary to develop a stronger digital culture to be able to analyze the main challenges provoked by the increasing use of connected objects (De Boever 2012). The CDA shows that a new public policy on IoT is about to be built in France. The problem in this context is the business model as most of the economic actors are start-ups that must have financial security for long-term projects. The risk for national authorities in European countries is that with the emergence of IoT, the start-ups might need to join bigger corporations. In other words, most of the start-ups working on the IoT could contribute to reinforce trust in transnational corporations. The roundtable of the Committee of Economic Affairs of the National Assembly was an opportunity

for successful leaders in this sector to claim lower taxes, and introduce more flexibility in economy. The digital entrepreneurs have more legitimacy to help politicians to implement policies that facilitate the emergence of data economy and digital innovation.

Recommendations

1. It is necessary to define a public agenda on the implementation of new digital policies. The state secretary of digital affairs should coordinate the follow up of the main digital policies with a specific parliamentary committee appointed for that. Digital innovation has a strong impact on the evolutions of societies, this is why governmental agencies should control these regulations. In other countries, a parliamentary committee could be appointed to evaluate the public policies on digital innovation with the presentation of a possible roadmap to the government.
2. It is important to make sure that debates on digital matters do not only promote successful stories in the IoT. The collection of best practices is limited if the reports and debates do not refer to failures. It would be valuable to tell stories that did not come true to study the real possibilities of this sector. The IoT is not science fiction, and a balanced point of view is required on this matter. The evaluation of the effects of IoT should tackle the challenges and the difficulties of such innovations. The parliamentary hearings should also invite actors that did not succeed in implementing long-term strategies with the IoT.
3. An independent national organization should be created to analyze the ethical consequences of political and technological innovations. In France, a specific committee of the National Assembly would elect the members of this organization for a period of three years. The reports of the organization would be discussed by the National Assembly. These organizations could also exist in other countries with a possible coordination to focus on the social consequences (social disrupture, education, …). An international structure could be created and associated with other multilateral arenas. It cannot be an NGO, as the dialogue with national organizations is political. The idea is not to diffuse best practices and recommendations, it is rather to coordinate national public policies to control the potential damages of such innovations.
4. The certification of new products in the IoT should be guaranteed to trace their evolution and their impact on society. The international organization would have a say on the certification of new products when they have ethical and social consequences.
5. The effects of lobbying should be minimized so that transnational corporations, alone, do not regulate the standard of innovations. Small-scale businesses should be empowered to avoid a concentration of power around transnational corporations in the field of IoT. In this perspective, the independent organizations on ethical issues should not be influenced by the lobbies.

References

Barley, S. R. (2007). Corporations, democracy, and the public good. *Journal of Management Inquiry, 16*, 201–215. https://doi.org/10.1177/1056492607305891.

Bauman, Z. (2005). *Liquid life*. Cambridge: Polity.

Borman, D. A. (2011). *Idolatry of the actual: Habermas, socialization and the possibility of autonomy*. New York: State University of New York Press.

Brown, J. S. (2004). *Storytelling in organizations: Why storytelling is transforming 21st century organizations and management*. Burlington: Butterworth-Heinemann.

Chaouchi, H. (Ed.). (2010). *The internet of things: Connecting objects to the web*. London: ISTE.

Corbett, A. C., & Katz, J. A. (2013). *Entrepreneurial resourcefulness: Competing with constraints*. Bradford: Emerald Group Publishing Limited.

Coskun, V., Ok, K., & Ozdenizci, B. (2011). *Near field communication (NFC)*. Hoboken: John Wiley & Sons.

Dearing, J. W., & Everett, M. R. (1996). *Agenda-setting*. Thousand Oaks: Sage.

De Boever, A. (2012). *Gilbert Simondon: Being and technology*. Edinburgh: Edinburgh University Press.

De Chanay, H. C., & Turbide, O. (2011). Les discours politiques. Approches interactionnistes et multimodales. Mots. *Les langages du politique*, 96. http://mots.revues.org/20170.

Dubey, G., & Moricot, C. (2016). *Dans la peau d'un pilote de chasse. Le spleen de l'homme-machine*. Paris: PUF.

Elden, S. (2006). Heidegger's animals. *Continental Philosophy Review, 39*, 273–291.

Eldred, M. (2009). *The digital cast of being: Metaphysics, mathematics, cartesianism, cybernetics, capitalism, communication*. Berlin: De Gruyter.

Erhel, C., & de La Raudière, L. (2017). *Rapport d'information n. 4362*. Paris: Assemblée Nationale.

Fairclough, N. (2001). Critical discourse analysis as a method in social scientific research. In R. Wodak & M. Meyer (Eds.), *Methods of critical discourse analysis* (pp. 121–138). London: Sage.

Fairclough, N. (2015). *Language and power*. London: Routledge.

Foucault, M. (1971). *L'ordre du discours*. Paris: Gallimard.

Foucault, M. (2010). *The government of self and others. Translated by Graham Burchell*. Basingstoke: Palgrave Macmillan.

Gibson, J. (1986). *The ecological approach to visual perception*. Hillsdale: Lawrence Erlbaum Associates.

Gillman, N. (2004). A jewish theology of death and the afterlife. In S. G. Post & R. H. Binstock (Eds.), *The fountain of youth* (pp. 94–108). Oxford: Oxford University Press.

Gimigliano, G. (Ed.). (2016). *Bitcoin and mobile payments constructing a European union framework*. London: Palgrave Macmillan.

Hauskeller, M. (2016). *Mythologies of transhumanism*. Cham: Springer International Publishing.

Heidegger, M. (1968). *What is a thing? Translated by WB Barton, Jr and V Deutsch*. Chicago: H. Regnery Co.

Heidegger, M. (1998). *Logik als Frage nach dem Wesen der Sprache. Gesamtausgabe 38, Vittorio*. Frankfurt am Main: Klostermann.

Jobert, B. (2004). Une approche dialectique des politiques publiques: l'héritage de *L'État en action*. *Pôle Sud, 21*, 43–54.

Koerten, K., & Veenswijk, M. (2013). Public sector information reuse across Europe: Patterns in policy-making from an organizational perspective. *Journal of E-Governance, 36*, 198–211.

Maingueneau, D. (1998). *Analyser les textes de communication*. Paris: Armand Colin.

March, J. (1962). The business firm as a political coalition. *Journal of Politics, 24*, 662–678.

Meyer, M. (2001). Between theory, method, and politics: Positioning of the approaches to CDA. In R. Wodak & M. Meyer (Eds.), *Methods of critical discourse analysis* (pp. 14–31). London: Sage.

Muller, P. (2009). *Les politiques publiques*. Paris: PUF.

Nownes, A. J. (2006). *Total lobbying*. New York: Cambridge University Press.
Ortolani, M. (2014). Extracting structured knowledge from sensor data for hybrid simulation. In S. Gaglio & G. L. Re (Eds.), *Advances onto the internet of things: How ontologies make the internet of things meaningful*. Cham: Springer International Publishing.
Padioleau, J. G. (1982). *L'État au concret*. Paris: PUF.
Paetz, P. (2014). *Disruption by design: How to create products that disrupt and then dominate markets*. Berkeley: Apress.
Passerini, K., El Tarabishy, A., & Patten, K. (2012). *Information technology for small business: Managing the digital enterprise*. New York: Springer.
Paveau, M. A. (2012). Ce que disent les objets. Sens, affordance, cognition. *Synergies Pays Riverains de la Baltique, 9*, 53–65.
Pinkard T (2012) Is recognition a basis for social or political thought? In: S O'Neill, NH Smith (eds.). Recognition theory as social research: Investigating the dynamics of social conflict. Palgrave Macmillan, Basingstoke: 21–38.
Pollitt, C., & Bouckaert, G. (2004). *Public management reform, a comparative analysis*. Oxford: Oxford University Press.
Premat, C. (2018). Can the French Republic be digital? Lessons from the last participatory experience on the law-making process. In J. Ramon Gil-Garcia, T. A. Pardo, & L. F. Luna-Reyes (Eds.), *Policy analytics, modelling and informatics: Innovative tools for solving complex social problems* (pp. 247–264). Cham: Springer.
Reich, R. (2007). *Supercapitalism: The transformation of business, democracy and everyday life*. New York: A. Knopf.
Salama, A. (2011). *Creating and re-creating corporate entrepreneurial culture*. Farnham: Ashgate Publishing Ltd.
Sethi, A. (2016). *The inside track of technology entrepreneurship*. Cham: Springer International Publishing.
Sennett, R. (2006). *The culture of the new capitalism*. Yale: Yale University Press.
Stiegler, B. (2013). *Automatic society: The future of work*. Cambridge: Polity.
Tardieu, L. (2005). La fonction entrepreneuriale dans la firme. *Revue d'économie industrielle., 109*(1), 119–137.
Thibault, F., & Mabi, C. (2015). Le politique face au numérique: une fascination à hauts risques. *Socio, 4*, 161–173.
Triantafillou, P. (2012). *New forms of governing: A Foucaldian inspired analysis*. Basingstoke: Palgrave Macmillan.
Weber, R. H., & Weber, R. (Eds.). (2010). *Internet of things: Legal perspectives*. Heidelberg: Springer.

Christophe Premat is an Associate Professor in Cultural Studies at the Department of Romance Studies and Classics and at the Centre for the Advancement for the University Teaching at Stockholm University. He is a member of the editorial board of the review Sens Public, an international web journal of social sciences. His current research focuses on the perception of participatory processes in the political discourse of French-speaking elites and the analysis of memory debates in France. He published in 2017 "Who killed whom? A comparison of political discussions about the genocide of 1915 in France and Sweden" (In: David Gaunt, Naures Atto, Sonder Onder Barthoma (eds.), Let them not return: Sayfo, the genocide of the Assyrian, Syriac and Chaldean Christians in the Ottoman Empire, New York: Berghahn Books: 233–253) and in 2016 "Acting and Thinking as a Revolutionary Organ: The Case of the French Review *Socialisme ou Barbarie* (1948–1965)", Journalism and Mass Communication, vol. 6, n. 9: 499–511.

He coedited, in 2015, a handbook on French–German relations, *Handwörterbuch der deutsch-französischen Beziehungen* (Nomos) and published, in 2014, a book entitled *L'idée d'une nouvelle représentation politique* (Edilivre).

Citizen Participation in Smart Government: A Conceptual Model and Two IoT Case Studies

Ali A. Guenduez, Tobias Mettler, and Kuno Schedler

Abstract In its simplest form, *smart government* can be understood as the combination of new technologies and organizational innovation strategies to further modernize the public sector. Within this development, the Internet of Things (IoT) often forms a key technological foundation, offering government authorities new possibilities for interaction with citizens and local communities. On the one hand, citizens can indirectly participate in governmental services' value creation by using public infrastructure or (un)knowingly sharing their data with the community. On the other hand, smart government initiatives may rely more intensively on citizens' active participation to improve public service delivery, increase trust in government actions, and strengthen community sentiment. In this chapter, we discuss active and passive participation scenarios of smart government initiatives and explain how sensor-based systems may enhance citizens' opportunities to participate in local governance. We present two practical cases from Switzerland demonstrating these two citizen involvement modes. We argue that active and passive participation of citizens and other stakeholders play a key role in generating necessary data for algorithmic decision-making to enable personalized interaction and real-time control of infrastructure in the future. We close with a discussion of the possibilities and boundaries of the IoT in the public sector and their possible influences on citizens' privacy and policy-making.

Keywords Participation · Smart government · Internet of things · IoT · Sensors · Big data · Algorithmic decision-making

A. A. Guenduez (✉) · K. Schedler
Smart Government Lab, Institute for Systemic Management and Public Governance, University of St. Gallen, St. Gallen, Switzerland
e-mail: aliasker.guenduez@unisg.ch; kuno.schedler@unisg.ch

T. Mettler
Swiss Graduate School of Public Administration, University of Lausanne, Lausanne, Switzerland
e-mail: tobias.mettler@unil.ch

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*, Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_9

Abbreviations

e-government	Electronic government
IoT	Internet of Things
IT	Information technology
LoRaWAN	Long-range wide area network
m-government	Mobile government

Introduction

Since the mid-1990s, efforts have been made to harness the Internet's potential for public administration (Caudle 1994; Lent 1995). Under the phrase *electronic government* (e-government), public administration digitalization has increased (Jaeger 2002). The main objectives of this first digitization stage included improving customer service, enhancing the efficiency and effectiveness of government actions, government accountability, transparency, and administrative management, and promoting citizen participation (Schedler et al. 2003; Yildiz 2007). This first e-government wave sought to create a digital environment in which public authorities provided services to their citizens electronically. However, since e-government has been introduced into public administration, it has been used primarily as a support tool for analogous and internal processes (Davison et al. 2005). There has been no fundamental change in the ways public administrations process their work, which has been particularly disappointing for citizens; their experiences when contacting governmental authorities have not fundamentally improved (Cohen 2006).

With the emergence of portable devices and the widespread availability of broadband wireless networks, the era of mobile government (*m-government*) sought to reduce this frustration and to address the growing demand for easy, effective, and convenient interaction with government agencies (Rossel et al. 2006). However, the paradigm shift from desktop to mobile has not always been successful, given that adjustments in attitudes, aspirations, skills, and behaviors were required from public administrators and citizens (Shareef et al. 2016). In many cases, m-government became synonymous with simply adapting the resolution of existing e-government websites to the smaller mobile device screens, without changing any other process parameters or service logics. Accordingly, the full potential of mobile technology was not used, rendering many m-government initiatives toothless. Positive effects on civic engagement and participation, as desired by government agencies, were seldom achieved (Albesher and Stone 2016).

However, in the past few years, we have seen some innovative, promising developments. Unlike previous e-government initiatives, many digital initiatives are now launched under the umbrella term *smart government,* with the purpose of establishing novel service delivery models by connecting physical, digital, public, and pri-

vate environments (Scholl and Scholl 2014; Bhatti et al. 2015; Rochet and Correa 2016). These new approaches take an important step further than past digitalization endeavors, asking how the relationship between administration and its stakeholders could be implemented in more efficient, effective, and/or unexpected ways using sensors, big data, and personalized algorithms (Bright and Margetts 2016). Fundamentally rethinking the ways governments operate is not only desirable but mandatory for smart government initiatives to be impactful and effective in establishing seamless information flows and collaborative decision-making (Chun et al. 2010) and, ultimately, more civic engagement and participation in community life (Sean et al. 2012).

Several authors have stressed the reinvigoration of government's use of new technological possibilities (Scholl and Scholl 2014; Anthopoulos 2017), particularly the Internet of Things (IoT) and related technologies, in order *"to interconnect and integrate information, processes, institutions, and physical infrastructure to better serve citizens and communities"* (Gil-Garcia 2012). Simply put, IT-induced change by public organizations based on emerging and advanced information technologies could lead to smarter and more engaged communities (Coe et al. 2001).

Similarly, Gil-Garcia (2012) defined smart government as the interplay of forward-looking technologies and organizational innovation in the public sector to improve interorganizational collaboration, information-sharing, and integration, with the goal of ultimately achieving a *smart state*. Mellouli et al. (2014) see smart government as an attempt to introduce new technologies for addressing innovative organizational usage cases, fulfilling e-government and m-government potential in openness, transparency, organizational renewal, and citizen participation. In this context, Harsh and Ichalkaranje (2015) emphasized the key role of data generated through new technologies and applications and a (machine-based and/or automatic) analysis for improving service delivery. According to them, the merging of new technological and organizational considerations would enable governments to transform e-government into smart government.

In our view, the IoT plays a vital role in the realization of smart government. Data obtained from everyday objects, such as smartphones, wearables, sensor-enabled devices, home appliances, surveillance cameras, or even vehicles (Zanella et al. 2014) provide unprecedented possibilities for government agencies to interact and build relationships with citizens and businesses (Janssen et al. 2017). The enormous amount and variety of data generated and autonomously distributed by such IoT objects could lead to *new services* for citizens, companies, and public administrations in numerous domains, such as public transportation and logistics, healthcare, urbanization, and/or the environment (Atzori et al. 2010).

However, in practice, many smart government initiatives often concentrate almost exclusively on technological aspects (Saunders and Baeck 2015), that is, the development of high-performance information and communication infrastructures. Examples include intelligent power grids for measuring and regulating the energy consumption of individual houses or entire localities, or intelligent parking space systems for managing the utilization of different parking facilities in a region or

municipality. A fundamental rethinking of government services and interaction patterns to become more citizen-centric is often missing. *Smartness* in such applications often means linking physical objects, such as waste containers, traffic lights, parking restrictions, and electricity meters, with public information infrastructure. This provides the foundation for automated data collection, data integration, and triggering simple tasks of control, regulation, or alerting, such as primitive, event-driven *if A, then B* procedures.

Certainly, smart government is more than just the introduction of a smarter IoT infrastructure to establish real-time control usage cases. If planned and managed carefully, it could foster more active citizens' participation in the value creation of governmental services. It could create an environment in which involvement and participation of the population in the public sphere (e.g., healthcare, security, transport) is deliberately encouraged so as to significantly enhance public service delivery, increase trust in government actions, and strengthen community sentiment. In this context, IoT would be indispensable for public administrations receiving sufficient detailed and contextualized information; this could serve as feedback for their planned and realized actions and could improve civic engagement. Several studies have shown that IoT applications could trigger and increase citizens' motivation to participate (Salim and Haque 2015; Nam and Pardo 2014).

We also focus on the *participation* aspect and enabling role of IoT in realizing the vision of smart government, since we consider it is a key success factor in democracies and modern public administrations. We start by discussing a conceptual model that illustrates different modes of participation in current smart government initiatives. Based on this description, we will then describe two case studies.

With the first case study, Smart City St. Gallen (a medium-sized municipality in the northeast of Switzerland), we delineate the *passive participation* mode, which is probably dominant in today's IoT implementations. As we will explain, *passive* in this scenario means that citizens are idle and take no deliberate actions to share data generated by IoT objects.

In the second case study, we showcase the DeSearch project, a joint effort by the Baden-Wuerttemberg Cooperative State University Ravensburg-Friedrichshafen (Germany) and the University of Lausanne (Switzerland) to develop a privacy-aware, patient-tracking solution based on *active participation* by concerned and/or affected citizens. In this scenario, *active* means that citizens must consciously decide whether or not to disclose IoT generated data. A high level of civic engagement is imperative to unlock the full potential of this smart government initiative.

Both case studies demonstrate a different logic that public administration must master so as to ensure that a smart government initiative is successful. This chapter closes with a discussion on smart government possibilities and boundaries in current practice, and their prospects to change citizens' privacy and public policy-making in the future.

Research Approach and Conceptualization of Citizen Participation in Smart Government Initiatives

The findings we presented are based on case study research. According to Robson (1993), this is a suitable empirical method for real-world research, enabling scientists to investigate a particular contemporary phenomenon in its real-life context using multiple sources of evidence, especially when the boundaries between a phenomenon and its context are not clear. Case studies involve an in-depth and close examination of one or multiple persons, organizations, communities, artifacts, or contemporary set of events (Stake 2006) to provide rich descriptions and develop (Eisenhardt 1989) or even test theories (Darke et al. 1998). One can differentiate between exploratory, descriptive, and explanatory research designs.

Case studies have proven to be an excellent method for exploring the duality of technology and social relationships (Myers 1997). In this context, they typically seek to answer *how* or *why* type questions, and are usually applied when a scientist has little or no control over a phenomenon, or when an inquiry addresses a situation in which there are many more variables of interest than data points (Yin 2009). To overcome this problem, scientists must rely on multiple sources of evidence; data must be triangulated.

Our research is an exploratory case study. To obtain the necessary data for this inquiry, we conducted participant observation and multiple expert interviews. Personal notes from field visits, communication material, technical documentation, and prototypes received from parties involved were additional sources for conclusions on the nature of participation in IoT-reliant smart government initiatives. We chose the selected cases according to the availability of technical experts as well as to represent the two extreme positions of active and passive participation.

Our starting point was a literature review on what is perceived as smart government. The broad consensus was that smart government initiatives can contribute significantly to the solution of a wide variety of current and future societal challenges (Gil-Garcia et al. 2014; Scholl and Scholl 2014). While such intelligent infrastructures can already address a multitude of everyday practical problems, such as saving electricity or optimizing traffic (Stankovic 2014), there is still a long way to go until we see the use of smart technologies in complex decision-making and context-aware reasoning (De Matos et al. 2017), such as the preparation of political mandates or the evaluation of state interventions.

Unfortunately, we found little evidence regarding the roles and conceptualizations of participation in the literature. Most papers on IoT in combination with smart government initiatives emphasized technical and operational aspects. However, many articles cited different buzzwords such as wiki government (Noveck 2009), crowdsourcing (Brabham 2010), open government (McDermott 2010), Government 2.0 (Nam 2012b, 2012a), or we-government (Linders 2012) to describe ways of cultivating open dialogue with and creating interest among citizens. While the literature suggests that active, involved citizens are better than passive, disinterested ones in democratic state governance (Putnam 1993), it offers little evidence on

how IoT could stimulate participation and lead to the purported effects. Analyzing and condensing the findings of our two case studies, we differentiated two perspectives—or modes—of participation, which we will briefly describe.

Mode I: Passive Participation

Most smart government initiatives underway today seek to use IoT for large-scale data collection to establish real-time control over dedicated aspects of public welfare. As we will detail in the subsequent case study of St. Gallen, citizens' roles in such a scenario are relatively passive. There is no need to take deliberate action or make decisions regarding data-sharing, and benefiting from these project types. They simply contribute to the overall data life cycle by using, or being surveyed, by those in public infrastructure. However, these "passively" generated data provide insights into the uses and effectiveness of services in key policy areas, such as transport, health, safety, and agriculture. The great advantage of this data type is that it represents real-time information, generating minimal costs. It provides a new basis for government and administrative decisions: simple, needs-based, and cost-effective regulation and control can be achieved.

Mode II: Active Participation

In contrast to the previous example—where IoT is used for large-scale data collection and automatizing simple control, regulation, or alerting tasks—there are also scenarios requiring a more interactive, joint creation of value between public agencies and citizens. Such smart government initiatives often seek to develop context-based decision-making tools and envision co-creation of public services that are supported by involved citizens. A major challenge in such scenarios is that active participation is quickly halted if the population is only seen as a data supplier (without providing personalized feedback or sensemaking about the real purpose of data-sharing), and the data flow necessary for the development of meaningful forecasts will diminish over time (Yassaee et al. 2016). Thus, it is important to inform and engage with citizens to ensure that the aims and data needs for an active smart government initiative are transparent. As we will show in the DeSearch case study, personal affection, concern, and solidarity could be reasons why citizens share their data.

Conceptual Model

Both modes of participation justify their existence, since they address dissimilar usage cases and fulfill very different public needs. Active and passive participation are not mutually exclusive; both can be combined in smart government initiatives, allowing more complex relationships to become visible. More precise knowledge about the efficiency and effectiveness of state measures can be gained by analyzing and evaluating such data that provides information about the public's behavior, as well as other trends (Mergel et al. 2016).

Accordingly, so that IoT-enabled smart government initiatives can reach their full potential, different elements must be considered and aligned. As shown in Fig. 1, we propose a conceptual model to approach smart government initiatives by applying a data life cycle perspective and concentrating on different modes of engaging with citizens.

To understand participation in IoT-reliant smart government initiatives, we must closely examine and understand the quality and origin of data sources. Smart government initiatives can use not only of public infrastructure (e.g., a city's camera surveillance system, weather and pollution sensors, and traffic light systems), but also private infrastructure for data collection and citizen participation; this is often forgotten. A large number of private data sources (e.g., smartphones, smartwatches, and micro-computers) can be systematically tapped (with citizens' unknowing consent) to obtain extremely detailed data about the habits, routines, and wishes of the

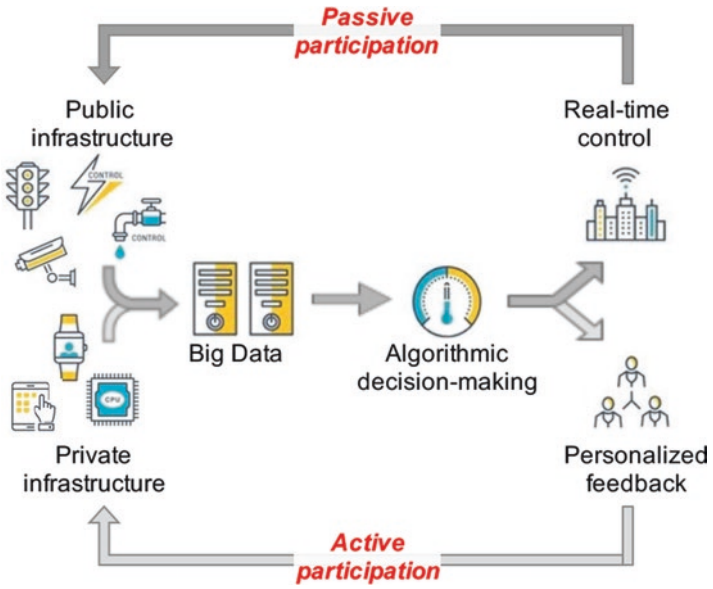


Fig. 1 Conceptual model describing active and passive citizen participation in smart government initiatives (translated from Guenduez et al. 2017)

population. Notably, smartness does not derive from data collection per se, or what many refer to as big data. In such applications, smartness lies in the context-related analysis and combination of a large amount of structured and unstructured data, which allows for self-learning algorithms to make increasingly precise statements about certain facts, groups, or even single individuals, enabling the automation or execution of certain tasks in much more efficient and citizen-friendly ways.

However, smart government initiatives should not end with data analysis and the prediction of events. To prevent the data life cycle from halting, government authorities must engage with citizens and must somehow pass the outcomes of algorithmic decision-making on to them.

We will now use two case studies to explain the differences between active and passive participation.

Passive Citizen Participation: The Smart City St. Gallen Case

To illustrate the passive participation mode in an IoT-enabled smart government initiative, we present the Smart City St. Gallen case.

St. Gallen in Switzerland is close to the borders of Germany, Austria, and Lichtenstein, and maintains close relationships with cities in these countries. St. Gallen is a suitable case for German-speaking countries to illustrate passive participation. From 2000 on, triggered by the Internet, the integration of citizens in the political process became increasingly articulated in public and political debate. As in many cities around the world, many of these e-government ideas have remained theoretical in St. Gallen and have still not become a reality (Baccarne et al. 2014).

The city made another attempt in 2015. The new initiative runs under the name Smart City St. Gallen and has reached significantly further than previous digitalization initiatives, recognizing the huge potential of IoT. The city does not limit the smart city concept to the application of current technologies, but pursues a holistic approach. St. Gallen's smart city strategy seeks to establish an ecologically sustainable and energy-efficient city. The city also seeks to enhance services for citizens, businesses, and other stakeholders through the use of IoT, sensors and data collection (St. Gallen 2016a).

St. Gallen is experimenting with a broad range of IoT technologies, such as smart metering, streetlights, parking, transportation, and waste management. Further, with the area-wide construction of a fiber-optic network, the city has established a "nervous system," enabling high-performance data networking. Having successfully accomplished the first pilot project in IoT applications, St. Gallen plans to extend the Long Range Wide Area Network (LoRaWAN) technology to the entire city. LoRaWAN is a wireless, low-power communication technology for IoT applications. St. Gallen is building on this infrastructure to exploit IoT technologies' potential: automatic collection of context-related data, integration into the overall system, and processing for real-time control. All these technologies are building the technological foundation of Smart City St. Gallen. Figure 2 illustrates how

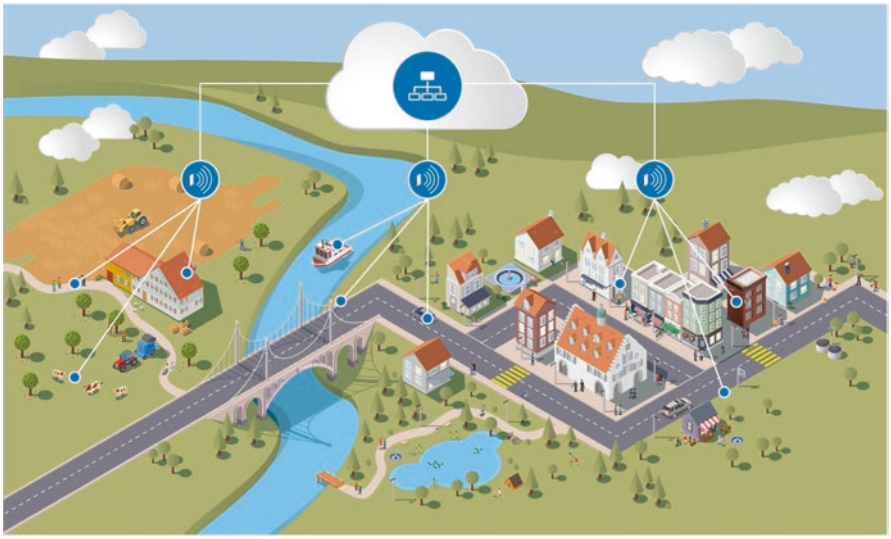


Fig. 2 The technological foundation of smart city St. Gallen (St. Gallen 2016a)

context-related data are automatically collected, integrated into the overall system, and processed for intelligent real-time control.

IoT located in the public infrastructure can create a participative environment (Kortuem et al. 2013). It offers a new opportunity for citizens to get involved in public services' governance. Citizen participation is not based on active expression of political will, but on their social participation in city life. We call this *passive participation*. By driving on a lit road, leaving a car in a parking space, using water, electricity or gas, or disposing waste, citizens communicate their needs to a certain extent through sensor systems. Real-time generated data from autonomous sources spread out through the public infrastructure illuminate a previously unknown volume, variety, and volatility of data about the use, efficiency, and effectiveness of services. Information gained from these data results in evidence-based governance in the truest sense of the word. Thus, citizens' passive involvement results in more citizen-centered governance of services. St. Gallen's IoT architecture is still under development. The experience gained in its smart city project is very promising. With this project's increasing maturity, government services will be better adapted to citizens' needs.

A concrete example of the passive participation cycle is the settlement project Sturzenegg. The city conducts the project to gain empirical civic experience with IoT technology. Sturzenegg has been in operation since mid-2017, installing gas, water, heat, and electricity sensors in the city. The sensors measure occupant consumption and transmit data via a fiber-optic network and LoRaWAN to central data centers, where they are linked, processed, and visualized by software. These data offer many benefits for the city and its citizens, allowing for an exact calculation of consumption. The city can react to bottlenecks in close to real-time. Linking the

data to an invoice system also allows for more efficient invoicing, which saves administrative costs. The data are fed back to the residents on an app provided by the city, so that each apartment can see its own current consumption and can adapt accordingly.

IoT enables St. Gallen to include everyone living and working in the city in the policy-making process. Foreigners, minors, and non-voters, who cannot or do not participate in the opinion-forming and decision-making processes, are becoming relevant actors. Sensors connected to parking spaces, street lighting, waste bins or water, gas, and electricity meters also collect data. With the integration of data, these sensors generate political opinion-forming and decision-making processes, and become part of value creation in government services. Thus, IoT not only enhances the quality of the public services, but also fosters a new form of interaction between politically unrepresented people and government. These people represent a large part of the population. Integration of this group into the political process via IoT infrastructure is a new way to promote democracy in cities.

IoT in public infrastructure has huge future potential; many applications are only beginning. The smart city strategy, in this first instance, seeks to modernize the city's infrastructure (water, gas, electricity, waste, traffic) via sensor systems, but needs to be developed further. A comprehensive implementation of IoT in the city is planned (St. Gallen 2016b). Today, St. Gallen is experimenting with the possibilities of IoT technology, knowing that smart IoT technologies alone do not guarantee smartness. Using the technologies to enhance government services is still in the concept stage. Once comprehensive IoT implementation in the city is complete, most data necessary to govern the city will be available via the sensor systems. Utilizing this information enables citizen-centered governance of government services and representation of all social groups in the political process.

Active Citizen Participation: The DeSearch Case

We present the DeSearch case as an example of active participation mode in an IoT-enabled smart government initiative.

For many years, local governments and the EC invested considerable financial resources into the development of assistive technologies for elderly people and others in need of increased care (Bächle et al. 2018), to improve their autonomy and wellbeing (Kubitschke et al. 2010). This is motivated by the fact that senior citizens living in homecare settings are much more independent and active (Sun et al. 2009; Mageroski et al. 2016) and generate a fraction of the costs of older people in long-term care facilities (Wimo et al. 2010). However, this has a downside; they are much more at risk of patient safety incidents (Tudor Car et al. 2017), which makes it crucial to research remote monitoring.

Sensor-based systems for patient monitoring have recently attracted much attention (Pantelopoulos and Bourbakis 2010). Via sensors and actuators integrated into clothing, shoes, bracelets, phones, watches, or integrated in smart home appliances,

it is possible to constantly track and accumulate significant biological, physical, behavioral, or environmental information (Swan 2013), which—if deliberately combined and designed with foresight—can be used to improve elderly persons' quality of life by enabling them to stay longer and more safely at home (Mileo et al. 2008).

DeSearch, a smart government project currently underway at the Baden-Wuerttemberg Cooperative State University Ravensburg-Friedrichshafen (Germany) and the University of Lausanne (Switzerland), seeks to develop privacy-aware means to track elderly persons and others in care without unnecessary surveillance and intervention in their daily lives (Bächle et al. 2016). Unlike existing GPS-based systems that record every step a person takes, DeSearch seeks to provide a much less intrusive solution that reduces stigmatization (Dahl and Holb 2012) and increases *adoption willingness*, particularly for persons with mild cognitive impairments, or those who only occasionally experience behavioral difficulties.

The DeSearch solution has several components (cf. Figure 3): (a) a button-sized Bluetooth transmitter that can easily be sewed into an elderly person's clothes or shoes, (b) a small receiver, and (c) a web application, all of which are used to help locate a missing person. Since DeSearch relies on Bluetooth technology, the system is also able to locate a person inside a building. This can be particularly handy in larger health institutions, such as metropolitan hospitals or care institutions, where there are countless spots to hide. However, a major downside compared to GPS-based solutions is its limited range of coverage, which led the research team to consider active participation of engaged citizens to counteract this issue. Figure 4 illustrates the basic functioning of DeSearch.

As noted, DeSearch does not permanently track a person's location. It can be activated when the individual passes a sensor barrier (e.g., a building's exits) or at

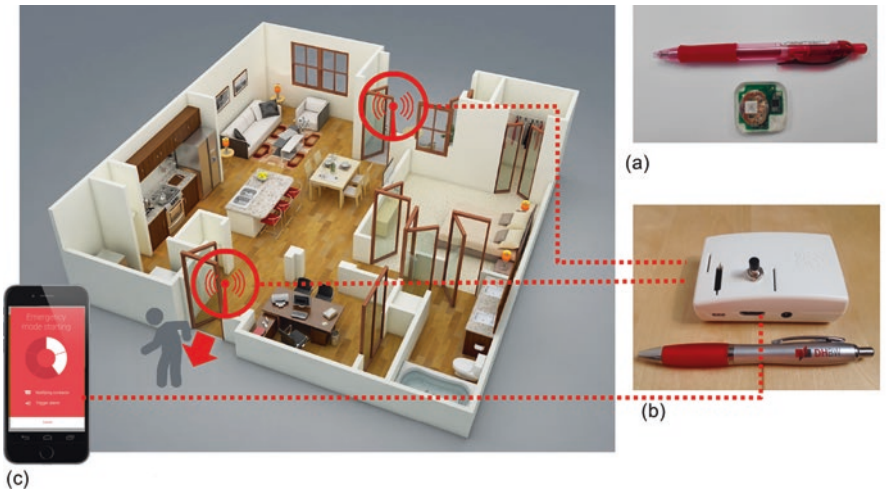


Fig. 3 The technological foundations of DeSearch. (**a**) DeSearch bluetooth-button. (**b**) DeSearch receiver. (**c**) DeSearch app

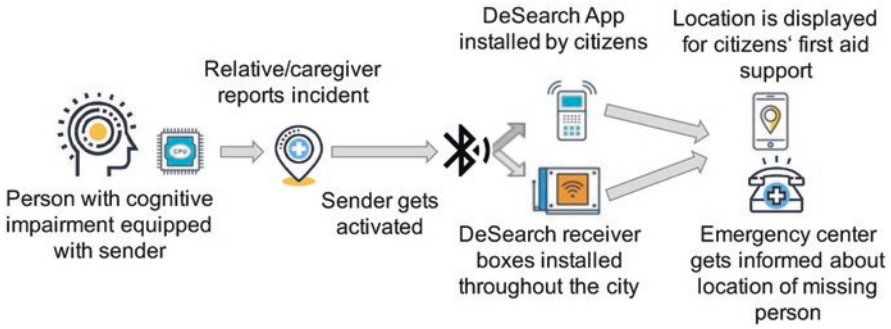


Fig. 4 Active citizen participation on DeSearch

the request of a relative or caregiver (e.g., if the subject is not immediately found in a designated room). To locate a person, DeSearch relies on two approaches.

Given that dementia patients' long-term memory is often good, they tend to go to certain locations (e.g., train stations, marketplaces, or bus stops) they remember. Thus, DeSearch intends to equip cities with a small number of low-cost receiver boxes (based on Raspberry Pi mini-computers) at possible locations, along with constantly moving receivers installed in public transportation vehicles or taxis. When a specific person is near a DeSearch receiver, the local emergency center is informed of their exact position.

An extension of coverage could come from actively involving concerned citizens. Many people know certain individuals or have family members with cognitive impairments. By installing the DeSearch app on their smartphones, the community can assist in locating missing persons. When turned on, a smartphone becomes a mobile receiving station, sharing private infrastructure to locate a missing person. The phone can also display a missing person's location to facilitate first-aid support. In sum, we define the deliberate and intentional participation in a smart government initiative—for example, sharing personal data and providing privately owned resources—as *active participation*.

Overall, active involvement could enhance public responsibility and could significantly minimize search costs for missing persons. In this case study, a network of engaged citizens is established (by running the DeSearch app in the background)—positive smart government.

Active participation creates new challenges for designers beyond the technical realization of IoT, because citizens must be convinced of a project's value. As with any surveillance and tracking technology, privacy concerns are key. Particularly in countries where there is a general distrust of government, there is a widespread conviction that government agencies repurpose one's personal infrastructure and information for objectives other than those initially promoted (Regan 2004; Mutimukwe et al. 2017). Many studies of privacy and information disclosure suggest that citizens perform a kind of cost-benefit analysis or *privacy calculus* (Dinev et al. 2016) to see whether the advantages of IoT-reliant government services are

worth the potential privacy risks of using these services. This is fundamentally different from the St. Gallen project, where usage is not a conscious decision, or where there is no real choice on how to access and receive a particular government service. Thus, a transparent and precise communication of costs and constraints of an IoT-reliant government service is needed, and could be a reasonable way to clarify the debate about winners and losers in data-based societies (Loebbecke and Picot 2015).

Key Learnings from these Two IoT Case Studies

Smart government is driven by the use of a new generation of ICT in the public sector. In contrast to previous digitization initiatives that focused on providing services via websites (Zakareya and Zahir 2005), smart government initiatives focus on the unprecedented possibilities and opportunities that new generation IoT technologies offer in collecting, connecting, analyzing, and sharing data—all in real-time, bridging digital and physical boundaries. The IoT will play a key role in the success of the smart government initiatives. Most importantly, IoT could raise the value creation process of government services by actively or passively including the entire population. In this sense, smart technologies are also social technologies, enabling the participation of large groups of people (Cardone et al. 2013). Participation in the value creation process is one a main principle of democracy, affording citizens opportunities to communicate information to government officials about their concerns and preferences (Verba et al. 1995).

We have discussed two modes of the inclusion of citizens in smart government: active and passive participation. Both modes depend on IoT-reliant scenarios. Through active and/or passive participation, citizens contribute to the provision of public services, as illustrated by these two practical cases.

The Smart City St. Gallen case study illustrates the potentials of IoT in public infrastructure, showing that smart infrastructures empower citizens by enabling them to influence government service provisions. As a driver on a smart lit road or a user of a public parking space with sensors, citizens become part of value creation in government services. Greater citizen involvement results in more citizen-centered governance of public services (Cooper et al. 2006), representing a service dimension of passive participation. It could embody a democratic dimension; public infrastructure not only integrates active citizens, but also foreigners, minors, and non-voters, who cannot or do not participate in political opinion-forming and decision-making processes.

The DeSearch case study illustrates how private infrastructures (smartphones) can be used for public tasks, such as for locating missing persons. This opens new possibilities, including privatization of public tasks. However, citizens' *participation motivation* cannot be taken for granted. Through positive stimuli (e.g., monetary incentives, public interest), citizens can be moved to augment or maximize their infrastructure. St. Gallen and DeSearch show that, by using private and public infrastructure, individuals or groups can actively and/or passively influence the provision

and governance of public services. Active and passive participation allow them to be part of the policy-making process and to enhance the quality of the public services they receive.

Active and passive participation have major consequences for public administration, enabling interaction with service providers, and influencing the provision and outcomes of public policies. Citizens are no longer only consumers, but become co-designers of and contributors to government services (Bertot et al. 2016; Uppström and Lönn 2017). Through the use of the public and/or private IoT infrastructure, citizens coproduce public services. Coproduction, as the process "through which inputs used to produce a good or service are contributed by individuals who are not 'in' the same organization" (Ostrom 1996). This means that it is not only government agencies who are providers of education, health, security, or infrastructure services, but also citizens and other stakeholders. Coproduction is not new to public administration; it has been at the heart of many previous attempts to include citizens in the policy cycle (Bovaird 2007; Bovaird et al. 2015; Fledderus et al. 2014). However, with IoT technologies, coproduction has a better chance to succeed under smart government (Van Waart et al. 2015). IoT creates an environment that strengthens citizens' roles as coproducers of public services (Schaffers et al. 2011), making it important to foster participative environments. Thus, constructing an open, public IoT infrastructure and encouraging citizens to use their private IoT infrastructure to cooperate with service providers are key to empowering citizens (Millard 2018).

Active and passive participation, as bottom-up approaches, counter the traditional, hierarchical relationship between a government (as service provider or guarantor) and the citizens (as users). A new conception of public service delivery is needed. The traditional, hierarchical model of government service delivery must be revised to account for IoT, sensor systems, and related developments, such as big data and algorithmic decision-making. Despite the potential of IoT, concerns about adverse effects abound. The growing skepticism regarding vanishing boundaries between what is private and what is public is a significant challenge. Trepidation about unauthorized access to private data, use of this data by government agencies for more than policy issues and it being another step toward government surveillance, is deeply rooted. *Smartness* in *smart government* means addressing these challenges while pursuing the benefits of the IoT.

Boundaries and Limitations of Smart Government

So far, we have emphasized numerous benefits of smart government. However, the concept also has limitations.

First, it is not easy to manage IoT-enabled smart government initiatives that connect physical, digital, public, and private environments. Smart governments place high demands on public decision makers, since they need to understand and control

the new technologies, implement them successfully in public administration, and add value to citizens. This requires technical, organizational, and managerial skills. Public administrations must acquire these capabilities.

Second, as noted, smart government has huge potential for democratic self-governance. However, this is not without risk. Public services in smart government rely on the collection and analysis of data derived from public and private infrastructures. Collecting and recording (personal) data raise a series of questions concerning privacy, which is fundamental to modern democracies. A lack of appropriate privacy norms poses a significant threat to democracy (Schwartz 1999). Smart governments need to empower citizens to control the collection, analysis, and dissemination of their personal data (Lessig 1999). Smart governments with inadequate personal data protection will have difficulties distancing themselves from a Big Brother reputation.

Third, smart technologies are at the core of smart government, enabling governments to become smart. Despite numerous benefits, there are big risks when governments rely exclusively on technology. Delegating routine administrative tasks to self-learning algorithms and the displacement of human control may have unintended consequences. As Bohn et al. (2004) note,

> Under "normal" circumstances, automated control processes increase system stability—machines are certainly much better than humans if they have to devote their whole attention to a particularly boring task. But situations that have not been anticipated in the software can easily have disastrous consequences if they are not directly controlled by humans.

Thus, smart governments need to develop control mechanisms for autonomous systems. Further, legal guidelines must be established in order to clarify accountability when things go wrong.

Fourth, by emphasizing active and passive participation in smart government, we have outlined the importance of a bottom-up approach. However, citizens often do not have the resources or are unwilling to participate without government intervention. To get citizens involved, governments need to incentivize the use of new technologies; it is hard for citizens to understand the possibilities of new technologies (Capdevila and Zarlenga 2015). As noted, through participation, citizens become co-designers of and contributors to government services. In case of a lack of participation, complementary top-down approaches in smart governments may be useful in order to provide services.

Fifth, our model, which demonstrates active and passive participation in smart government, is a strong simplification of realities. The advantage of our model is that it can be used in different contexts, but it does not reveal all the details to be found in smart government initiatives. Our model is descriptive; it does not allow for statements about causalities. It does not explain how and why citizens participate. However, this simplicity allows for a wide range of applications. The elements of the model point to relevant aspects of smart government, enabling a structured analysis and discourse, which has merits.

Practical Implications

We conclude by pointing out some practical implications. First, merely providing public infrastructure with sensors is not enough. For municipalities to generate added value, they must be linked to citizens' private infrastructures. Citizens should be able to access city services at any time with their smart devices; only then do they become coproducers of services.

Second, a smart city is a connected city; the same is true for any other smart government initiative (Dais et al. 2008). The individual data generated by sensors must be linked, so that government services that use these data can achieve remarkable public value for citizens. For instance, this would mean linking movement data collected by street lighting with data from car park sensors (or even from parked cars themselves), to reduce a city's energy consumption, thereby minimizing costs for the public, as well as lowering the light pollution that affects animals in city surroundings. This could also have practical benefits, such as estimating parking space occupancy. In the St. Gallen case, a link between sensors and smart services is not yet in place. St. Gallen is not alone in this regard. In many smart government initiatives, data collection and use still take place in silos. Public managers must understand that such projects are in most instances coproduction initiatives (Paskaleva et al. 2018). Collaboration with a multitude of stakeholders is needed, whether with other government authorities, private companies, or as we have highlighted, with citizens themselves.

Third, smart government initiatives only work if citizens participate (Anttiroiko et al. 2014). They do this when they understand how smart services, sensors, and data generated from IoT devices are collected, stored, and analyzed, as well as what public value may be achieved by these measures. A concrete, open information policy can encourage more active citizen participation. Collecting data for the sake of collecting, as often happens, will lead to resistance from citizens. Because coproduction is key for the presented participation data life cycle to continue, we advise public managers to carefully consider this.

Fourth, public administration must be aware that the sample from which they draw their conclusions could be biased (Ignacio et al. 2017). Data from active and passive participation are not necessarily representative of the entire population; biased participation leads to biased data and therefore to biased services. For instance, if only certain neighborhoods are equipped with sensors, the collected data do not allow for extrapolation to the entire city population. This is the same for active participation, since disadvantaged groups of the population participate less than others (Warren 2007). As a result, public policies formed by these data may be biased and may favor those who leave digital footprints, excluding those who do not participate. Thus, smart governments are advised to also focus on persons who leave no digital footprint.

Finally, with such a wealth of possible data sources, it becomes important for smart governments to distance themselves from any Big Brother or *uberveillance* mentality (Michael et al. 2014). Quality should come before quantity. Collecting as

much data as possible does not necessarily mean providing better services. Only data that are needed to improve services to citizens should be collected. Sensors and IoT are not an end but a means to an end.

Acknowledgments The authors are grateful to Prof. Dr. Michael Bächle, Prof. Dr. Stephan Daurer, and Prof. Dr. Andreas Judt of the Baden-Wuerttemberg Cooperative State University Ravensburg-Friedrichshafen, as well as to Dr. Christian Geiger (Chief Digital Officer, City of St. Gallen) and research assistant Michel Schibler (University of St. Gallen).

References

Albesher, A. S., & Stone, R. T. (2016). Current state of m-government research: Identifying future research opportunities. *International Journal of Electronic Governance, 8*(2), 119–139.

Anthopoulos, L. G. (2017). Smart government: A new adjective to government transformation or a trick? In *Understanding smart cities: A tool for smart government or an industrial trick?* (pp. 263–293). Cham: Springer.

Anttiroiko, A.-V., Valkama, P., & Bailey, S. J. (2014). Smart cities in the new service economy: Building platforms for smart services. *AI & SOCIETY, 29*(3), 323–334.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Baccarne, B., Mechant, P., & Schuurman, D. (2014). Empowered cities? An analysis of the structure and generated value of the smart city Ghent. In R. P. Dameri & C. Rosenthal-Sabroux (Eds.), *Smart city* (pp. 157–182). Cham: Springer.

Bächle, M., Daurer, S., Judt, A., & Mettler, T. (2016). iCare—Supporting people with increased need for care with smart and mobile it. *European Journal of Epidemiology, 31*(Supplement 1), S34–S34.

Bächle, M., Daurer, S., Judt, A., & Mettler, T. (2018). Assistive technology for independent living with dementia: Stylized facts and research gaps. *Health Policy and Technology, 7*(1), 98–111. *forthcoming*.

Bertot, J., Estevez, E., & Janowski, T. (2016). Universal and contextualized public services: Digital public service innovation framework. *Government Information Quarterly, 33*(2), 211–222.

Bhatti, Z. K., Kusek, J. Z., & Verheijen, T. (2015). *Logged on: Smart government solutions from South Asia*. Washington, DC: World Bank.

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., & Rohs, M. (2004). Living in a world of smart everyday objects - social, economic, and ethical implications. *Human and Ecological Risk Assessment, 10*(5), 763–785.

Bovaird, T. (2007). Beyond engagement and participation: User and community coproduction of public services. *Public Administration Review, 67*(5), 846–860.

Bovaird, T., Van Ryzin, G. G., Loeffler, E., & Parrado, S. (2015). Activating citizens to participate in collective co-production of public services. *Journal of Social Policy, 44*(1), 1–23.

Brabham, D. C. (2010). Moving the crowd at threadless: Motivations for participation in a crowdsourcing application. *Information Communication & Society, 13*(8), 1122–1145.

Bright, J., & Margetts, H. (2016). Big data and public policy: Can it succeed where e-participation has failed? *Policy and Internet, 8*(3), 218–224.

Capdevila, I., & Zarlenga, M. I. (2015). Smart city or smart citizens? The Barcelona case. *Journal of Strategy and Management, 8*(3), 266–282.

Cardone, G., Foschini, L., Bellavista, P., Corradi, A., Borcea, C., Talasila, M., et al. (2013). Fostering participaction in smart cities: A geo-social crowdsensing platform. *IEEE Communications Magazine, 51*(6), 112–119.

Caudle, S. L. (1994). *Reengineering for results : Keys to success from government experience*. Washington, D.C.: Center for Information Management, National Academy of Public Administration.

Chun, S., Shulman, S., Sandoval, R., & Hovy, E. (2010). Government 2.0: Making connections between citizens, data and government. *Information Polity, 15*, 1, 2), 1–1, 2), 9.

Coe, A., Paquet, G., & Roy, J. (2001). E-governance and smart communities - a social learning challenge. *Social Science Computer Review, 19*(1), 80–93.

Cohen, J. E. (2006). Citizen satisfaction with contacting government on the internet. *Information Polity, 11*(1), 51–65.

Cooper, T. L., Bryer, T. A., & Meek, J. W. (2006). Citizen-centered collaborative public management. *Public Administration Review, 66*(s1), 76–88.

Dahl, Y., & Holb, K. (2012). *Value biases of sensor-based assistive technology: Case study of a gps tracking system used in dementia care*. Paper presented at the Designing Interactive Systems Conference, Newcastle Upon Tyne, UK.

Dais, A., Nikolaidou, M., Alexopoulou, N., & Anagnostopoulous, D. (2008). Introducing a public agency networking platform towards supporting connected governance. In M. A. Wimmer, H. J. Scholl, & E. Ferro (Eds.), *Electronic government* (pp. 375–387). Berlin: Springer.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigour, relevance and pragmatism. *Information Systems Journal, 8*(4), 273–289.

Davison, R. M., Wagner, C., & Ma, L. C. (2005). From government to e-government: A transition model. *Information Technology & People, 18*(3), 280–299.

de Matos, E., Amaral, L. A., & Hessel, F. (2017). Context-aware systems: Technologies and challenges in internet of everything environments. In J. M. Batalla, G. Mastorakis, C. X. Mavromoustakis, & E. Pallis (Eds.), *Beyond the internet of things: Everything interconnected* (pp. 1–25). Cham: Springer.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In *Advances in healthcare informatics and analytics* (pp. 19–50). New York: Springer.

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review, 14*(4), 532–550.

Fledderus, J., Brandsen, T., & Honingh, M. (2014). Restoring trust through the co-production of public services: A theoretical elaboration. *Public Management Review, 16*(3), 424–443.

Gil-Garcia, J. R. (2012). Towards a smart state? Inter-agency collaboration, information integration, and beyond. *Information Polity, 17*(1), 269–280.

Gil-Garcia, J. R., Helbig, N., & Ojo, A. (2014). Being smart: Emerging technologies and innovation in the public sector. *Government Information Quarterly, 31*, I1–I8.

Guenduez, A. A., Mettler, T., & Schedler, K. (2017). Smart government – Partizipation und empowerment der Bürger im Zeitalter von big data und personalisierter Algorithmen [smart government – Participation and empowerment of citizens in the era of big data and personalized algorithms]. *HMD Praxis der Wirtschaftsinformatik, 54*(4), 477–487.

Harsh, A., & Ichalkaranje, N. (2015). Transforming e-government to smart government: A south Australian perspective. In L. C. Jain, S. Patnaik, & N. Ichalkaranje (Eds.), *Intelligent computing, communication and devices* (pp. 9–16). New Delhi: Springer.

Ignacio, C. J., Francisco, R.-M., & Ramon, G.-G. J. (2017). Enacting social media success in local public administrations: An empirical analysis of organizational, institutional, and contextual factors. *International Journal of Public Sector Management, 30*(1), 31–47.

Jaeger, P. T. (2002). Constitutional principles and e-govemment: An opinion about possible effects of federalism and the separation of powers on e-govemment policies. *Government Information Quarterly, 19*(4), 357–368.

Janssen, M., Konopnicki, D., Snowdon, J. L., & Ojo, A. (2017). Driving public sector innovation using big and open linked data (BOLD). *Information Systems Frontiers, 19*(2), 189–195.

Kortuem, G., Bandara, A. K., Smith, N., Richards, M., & Petre, M. (2013). Educating the internet-of-things generation. *Computer, 46*(2), 53–61.

Kubitschke, L., Cullen, K., & Müller, S. (2010). *ICT & ageing: European study on users, markets and technologies – Final report*. Brussels: European Commission.

Lent, M. (1995). *Government online*. New York, NY: Harper Perennial.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York NY: Basic Books.

Linders, D. (2012). From e-government to we-government: Defining a typology for citizen coproduction in the age of social media. *Government Information Quarterly, 29*(4), 446–454.

Loebbecke, C., & Picot, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *The Journal of Strategic Information Systems, 24*(3), 149–157.

Mageroski, A., Alsadoon, A., Prasad, P. W. C., Pham, L., & Elchouemi, A. (2016). *Impact of wireless communications technologies on elder people healthcare: Smart home in australia.* Paper presented at the 13th International Joint Conference on Computer Science and Software Engineering, Khon Kaen, Thailand.

McDermott, P. (2010). Building open government. *Government Information Quarterly, 27*(4), 401–413.

Mellouli, S., Luna-Reyes, L. F., & Zhang, J. (2014). Smart government, citizen participation and open data. *Information Polity, 19*, 1), 1–1), 4.

Mergel, I., Rethemeyer, R. K., & Kimberley, I. (2016). Big data in public affairs. *Public Administration Review, 76*(6), 928–937.

Michael, M., Michael, K., & Perakslis, C. (2014). *Uberveillance and the internet of things and people.* Paper presented at the IEEE International Conference on Contemporary Computing and Informatics Mysore, India.

Mileo, A., Merico, D., & Bisiani, R. (2008). *Wireless sensor networks supporting context-aware reasoning in assisted living.* Paper presented at the 1st International Conference on Pervasive Technologies related to Assistive Environments, Atherns, Greece,

Millard, J. (2018). Open governance systems: Doing more with more. *Government Information Quarterly, 35*(4), S77–S87. *forthcoming*.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2017). *Trusting and adopting e-government services in developing countries? Privacy concerns and practices in rwanda.* Paper presented at the International Conference on Electronic Government, Lyon, France.

Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly, 21*(1), 241–242.

Nam, T. (2012a). Citizens' attitudes toward open government and government 2.0. *International Review of Administrative Sciences, 78*(2), 346–368.

Nam, T. (2012b). Suggesting frameworks of citizen-sourcing via government 2.0. *Government Information Quarterly, 29*(1), 12–20.

Nam, T., & Pardo, T. A. (2014). The changing face of a city government: A case study of Philly311. *Government Information Quarterly, 31*, S1–S9.

Noveck, B. S. (2009). *Wiki government: How technology can make government better, democracy stronger, and citizens more powerful* (pp. 1–224). Washington: Brookings Institution Press.

Ostrom, E. (1996). Crossing the great divide: Coproduction, synergy, and development. *World Development, 24*(6), 1073–1087.

Pantelopoulos, A., & Bourbakis, N. G. (2010). A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews, 40*(1), 1–12.

Paskaleva, K., Cooper, I., & Concilo, G. (2018). Co-producing smart city services: Does one size fit all? In R. Bolívar & M. Pedro (Eds.), *Smart technologies for smart governments: Transparency, efficiency and organizational issues* (pp. 123–158). Cham: Springer.

Putnam, R. D. (1993). *Making democracy work. Civic traditions in modern Italy*. Princeton: Princeton University Press.

Regan, P. M. (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly, 21*(4), 481–497.

Robson, C. (1993). *Real world research: A resource for social scientists and practitioner-researchers*. Oxford: Blackwell.

Rochet, C., & Correa, J. D. P. (2016). Urban lifecycle management: A research program for smart government of smart cities. *Revista de Gestão e Secretariado, 7*(2), 1–20.

Rossel, P., Finger, M., & Misuraca, G. (2006). " Mobile" e-government options: Between technology-driven and user-centric. *Electronic Journal of E-Government, 4*(2), 79–86.

Salim, F., & Haque, U. (2015). Urban computing in the wild: A survey on large scale participation and citizen engagement with ubiquitous computing, cyber physical systems, and internet of things. *International Journal of Human-Computer Studies, 81*, 31–48.

Saunders, T., & Baeck, P. (2015). *Rethinking smart cities from the ground up*. London: Nesta.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation. *The Future Internet*, 431–446.

Schedler, K., Summermatter, L., & Schmidt, B. (2003). *Electronic government einführen und entwickeln. Von der Idee zur praxis [introducing and developing electronic government. From the idea to the practice]*. Bern: Paul Haupt.

Scholl, H. J., & Scholl, M. C. (2014). *Smart governance: A roadmap for resarch and practice.* Paper presented at the Proceedings of the 2014 iConference, Berlin.

Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review, 52*(6), 1609-+.

Sean, W., Robert, A. P., & Thomas, G. (2012). Value co-creation through collective intelligence in the public sector: A review of us and european initiatives. *Vine, 42*(2), 251–276.

Shareef, M. A., Kumar, V., Dwivedi, Y. K., & Kumar, U. (2016). Service delivery through mobile-government (mgov): Driving factors and cultural impacts. *Information Systems Frontiers, 18*(2), 315–332.

St. Gallen (2016a). St. Gallen ist bereit für das “Internet der Dinge” [St. Gallen is ready for the “Internet of Things”]. http://www.stadt.sg.ch/news/14/2016/07/internet-der-dinge-st-gallen.mobileView.html.

St. Gallen (2016b). Vorlage Stadtparlament. Smartnet: Immissionsarmes Funknetz als Ergänzung zum Glasfasernetz zur Realisierung eines “Internet of Things” in der Stadt St. Gallen [bill to the city parliament: Smartnet: Low-immission wireless network as a supplement to the fiber-optic network for the realization of “internet of things” in the city of St. Gallen]. https://www.stadt.sg.ch/news/14/2016/07/internet-der-dinge-st-gallen/_jcr_content/Par/downloadlist/DownloadListPar/download_5.ocFile/Smartnet%20Immissionsarmes%20Funknetz%20als%20Ergänzung%20zum%20Glasfasernetz%20zur%20Realisierung%20eines%20Internet%20of%20Things%20in%20der%20Stadt%20St.Gallen.pdf.

Stake, R. E. (2006). *Multiple case study analysis*. New York: The Guilford Press.

Stankovic, J. A. (2014). Research directions for the internet of things. *IEEE Internet of Things Journal, 1*(1), 3–9.

Sun, H., De Florio, V., Gui, N., & Blondia, C. (2009). *Promises and challenges of ambient assisted living systems.* Paper presented at the 6th International Conference on Information Technology: New Generations, Las Vegas, USA.

Swan, M. (2013). The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data, 1*(2), 85–99.

Tudor Car, L., El-Khatib, M., Perneczky, R., Papachristou, N., Atun, R., Rudan, I., et al. (2017). Prioritizing problems in and solutions to homecare safety of people with dementia: Supporting carers, streamlining care. *BMC Geriatrics, 17*(26), 1–8.

Uppström, E., & Lönn, C.-M. (2017). Explaining value co-creation and co-destruction in e-government using boundary object theory. *Government Information Quarterly, 34*(3), 406–420.

van Waart, P., Mulder, I., & de Bont, C. (2015). A participatory approach for envisioning a smart city. *Social Science Computer Review, 34*(6), 708–723.

Verba, S., Schlozman, K. L., & Brady, H. E. (1995). *Voice and equality: Civic voluntarism in american politics*. Cambridge: Harvard University Press.

Warren, M. (2007). The digital vicious cycle: Links between social disadvantage and digital exclusion in rural areas. *Telecommunications Policy, 31*(6), 374–388.
Wimo, A., Jönsson, L., & Winblad, B. (2010). Health economic aspects of dementia. In D. Ames, A. Burns, & J. O'Brien (Eds.), *Dementia* (4th ed., pp. 327–340). Boca Raton: CRC Press.
Yassaee, M., Mettler, T., & Winter, R. (2016). *Using affordance analysis to design individual analytics ecosystems*. Rüschlikon: Swiss Re Centre for Global Dialogue.
Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly, 24*(3), 646–665.
Yin, R. K. (2009). *Case study research* (4thed. ed.). Los Angeles: Sage.
Zakareya, E., & Zahir, I. (2005). E-government adoption: Architecture and barriers. *Business Process Management Journal, 11*(5), 589–611.
Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.

Ali A. Guenduez is Assistant Professor of Digital Government and Head of Smart Government Lab at the University of St.Gallen. His research interests include technology adoption, digital transformation, public sector innovation and smart government.

Tobias Mettler is Associate Professor at the Swiss Graduate School of Public Administration, University of Lausanne. His research interests are in the area of design science research, technology adoption, applications of data science, and business models, with a particular focus on public sector innovation.

Kuno Schedler is Full Professor at the University of St.Gallen. He teaches Public Management and Organization Theory. His main research areas are accounting and controlling in the public sector, general management in public administration, public governance and corporate governance, multirational management, electronic government, and smart government.

Index

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*,
Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8