Special track at the 13th *Philosophy of Management* conference
University of Greenwich, 25-28 June 2018

Eda Keskin

Abstract Submission

Title of Abstract: Responsible Innovation and Smart Cities

In this paper, I will address the concept of ethical responsibility in a case of innovation posing unknown and unintended consequences. In this context, ethical considerations surrounding individual privacy and other potential concerns regarding the technologies that comprise smart cities will be discussed.

The concept of the smart city is one that integrates traditional infrastructure and new information and communication technologies that proposes to create "an entire system for resource-efficient and real time city-related service providing in urban environments" (AlDairi & Lo'ai, 2017, p. 1087). Five main components of smart cities are modern information and communication technologies, buildings, utilities and infrastructure, transportation and traffic management and the city itself. It works through "cooperation between governance institutes and public and private foundations to implement and deploy long-term computerized platforms that impose using modern technologies including mobile cloud computing, electronic objects, networks and intelligent decision-making methodologies" (AlDairi & Lo'ai, 2017, p. 1087). AlDairi and Lo'ai examine security and privacy in smart cities as they deem these factors pose critical challenges which may cause harm if they are not properly considered. AlDairi and Lo'ai emphasize information and network protection from malicious activities and that data privacy is a main concern: "By data security, we mean data tendency to be accidentally or intentionally affected by technical failures caused by attacks or malicious activities; and by data privacy, we mean the ability to protect data from unauthorized accessing or re-using in addition to protect their collection processes and all operations being run on them" (AlDairi & Lo'ai, 2017, pp. 1087-1088). Smart cities can provide many benefits to their inhabitants. However, there exists concern regarding data privacy as it is transferred over non-secure channels. Therefore, it is crucial to secure communication channels as it passes over wireless networks. It is "important to alert planners and analysts for the necessity of thinking about protection against security vulnerabilities during the design of smart city" (AlDairi & Lo'ai, 2017, p. 1088).

René von Schomberg describes responsible research and innovation (RRI) should be understood as "a strategy of stakeholders to become mutually responsive to each other, anticipating research and innovation outcomes aimed at the 'grand challenges' of our time, for which they share responsibility" Schomberg, 2013). Blok and Lemmens assert that these "grand chal-

lenges“of our time include climate change, resource depletion, poverty alleviation, ageing societies, etc. (von Schomberg 2013). (Blok & Lemmens, 2015, p. 21).

Responsible research and innovation (RRI) implies the introduction of broader foresight and impact assessments for new technologies beyond their anticipated market-benefits and risks (von Schomberg, 2013). Blok and Lemmens argue that “responsibility is conceptualized “as an *add-on* or extension to the concept of innovation; responsible innovation = regular innovation + stakeholder involvement with regard to ethical and societal aspects. With the help of this extension, innovation processes will be better enabled to balance economic (profit), sociocultural (people) and environmental (planet) interests” (Blok & Lemmens, 2015, p. 20). One of the problems of innovation in smart cities is that people as individuals cannot take part in the innovation process as stakeholders when it comes to data collection belonging to individuals.

Another problem would be the crucial differences between the stakeholders:

> “Profit and nonprofit organizations have divergent approaches to value creation; companies will naturally focus on economic value creation by producing and selling products and services, while NGOs for instance will focus on social value creation by advocating social norms and values (Yaziji and Doh 2009; cf. Bos et al. 2013). Because of these differences between various stakeholders, actual efforts to involve stakeholders in innovation processes are liable to failure” (Blok & Lemmens, 2015, p. 22).

Conditions of transparency amongst stakeholders makes data collection in smart cities especially problematic. “Although transparency towards stakeholders is a necessary condition of open innovation processes, the call for a mutual responsiveness among stakeholders—i.e. the reduction of information asymmetries—in the responsible innovation literature is highly naive. For this reason, collaborations with stakeholders are sometimes explicitly restricted, especially in case of intellectual property (IP) and secrecy (Flipse 2012)” (Blok & Lemmens, 2015, p. 24). Therefore, another reason “to question the possibility of responsible innovation is that the ‘transparency’ and ‘mutuality’ among stakeholders is limited” (Blok & Lemmens, 2015, p. 25).

Smart city technologies generally have been argued for by highlighting management and environmental benefits and in the development of new markets. However, the risks of this new technology when it comes to data collection and power structures may have not been discussed properly. AlDairi and Lo’ai mention that data security in smart cities is quite tricky and challenging as it “implicates high level of dependency and connectivity across its layers (data/information, technology, application, and infrastructure)” (AlDairi & Lo’ai, 2017, p. 1089). AlDairi and Lo’ai see specific danger in using cameras in smart cities: “cities are full of private and public cameras which both are protected variably using encryption protection and username/password protection. Reaching private or public cameras and having access on them cause violation to individuals’ privacy and spying on governmental concerns” (AlDairi & Lo’ai, 2017, p. 1089). Privacy is a paramount topic when it comes to possible violations:

> "Privacy is ensured by protecting five privacy related issues: protecting identities that indicate protecting personnel and their confidential data; protecting people areas that indicate to protect each one's space and properties; protecting locations which indicate preventing spatial tracking; communication protection which indicate not to eavesdrop any kind of conversations; and finally, transactions protection that protect every single purchase, exchange and query" (AlDairi & Lo'ai, 2017, p. 1090).

Similarly, the European Commission's 'Science in Society' program focuses on "citizen engagement and participation of societal actors in research and innovation" (EC, 2013a) (Pellé & Reber, 2015, p. 110). In the case of smart cities and data collection of individuals it is almost inappropriate and impossible to enable citizen engagement as was possible previously. People's responses to smart cities show that a high percentage feel that these cities are vulnerable to cyber attack. Matter discusses the issue of trust in that "lack of trust makes it difficult for governments and businesses to persuade citizens that the science and technology choices they fund are for the public good and not simply for financial or personal gain and new approaches are needed to involve all groups in thinking through the choices and the decisions that are made" (Matter, 2011, p. 6). Actually, governance in science has evolved to include some public concerns. However, science governance still struggles "to be adaptive and responsive to public values, to the social and ethical impacts of science, and to the inherent complexity and uncertainty of natural and social systems in late modernity" (Beck, 2000; Felt and Wynne, 2007; Funtowicz and Ravetz, 1993) (Macnaghten & Chilvers, 2014, p. 530).

Helpnet Security reports that ninety-eight percent of respondents to a survey conducted by Dimensional Research believe that smart cities are at risk for cyber attacks (Help Net Security, 2016). The problem is that cyber security in smart cities is highly complex. "Mainly cyber security is affected by the emergent integration of technologies and the resulted intensive communication, high complexity and high interdependency, which leads to unbounded attack surface and cryptography-related issues" (AlDairi & Lo'ai, 2017, p. 1090). Help Net Securityn reports that smart cities use IT solutions which include smart grids, transportation, surveillance cameras, wastewater treatment which all face cyber threats. Andrew Ginter, VP Industrial Security at Waterfall Security Solutions, told Help Net Security:

> "A lot of people are talking about privacy threats in smart cities and the Internet of Things. Nobody is talking about safety, or the reliability of physical infrastructure essential to public safety. Nobody is going to care about a privacy leak if they have no power, or no clean water for weeks. There is no widespread understanding of the difference between monitoring and control. Both are "data." Privacy is the big risk with monitoring. Safety is the big risk with control" (Help Net Security, 2016).

Sixty-one percent of respondents answering the question as to why there is a lack of cyber security resources for smart city initiatives cited budgets and sixty percent believe politics in-

terfere with decision-making. Twenty-six percent answered that transportation faced the greatest cyber security risks in comparison to other smart city services. Ninety-eight percent declared that in their jurisdictions, smart city initiatives are important (Help Net Security, 2016).

Smart cities are dependent on machine-to-machine (M2M) interactions and decision-making. In addition to the fact that M2M decision-making (M2MD) is a beneficial feature, it becomes one of the greatest risks (Reys, 2016). Rambus lists the possible attacks to a smart city: 1) "**Man-in-the-middle**: An attacker breaches, interrupts or spoofs communications between two systems." 2) "**Data & identity theft**: Data generated by unprotected smart city infrastructure such as parking garages, EV charging stations and surveillance feeds provide cyber attackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identify theft." 3) **Device hijacking**: The attacker hijacks and effectively assumes control of a device." 4) "**Distributed Denial of Service (DDoS)**: A denial-of- service attack (DoS attack) attempts to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet." 5) "**Permanent Denial of Service (PDoS)**: Permanent denial- of-service attacks (PDoS), also known loosely as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware" (Rambus, 2017).

In conclusion, there are "'epistemic' factors such as the inherent complexity, uncertainty and unpredictability of technological innovation on the one hand and 'moral' and 'political' factors like conflicting worldviews, interests and value systems among stakeholders and power imbalances on the other." (Blok & Lemmens, 2015, p. 31). The practical applicability of responsible innovation for smart cities is questionable; however it offers a framework to open questions and includes the public as a stakeholder in decision giving processes.

Keywords: responsible innovation, innovation management, engineering ethics, smart cities, privacy, security, stakeholders, public concern, trust

References

Blok Vincent, Lemmens Pieter, "The Emerging Concept of Responsible Innovation. Three Reasons Why It is Questionable and Calls for a Radical Transformation of the Concept of Innovation", in Responsible Innovation 2 Concepts, Approaches and Applications. Koops**,** B.-J., Oosterlaken, I., Romijn, H., Swierstra**,** T., van den Hoven, J. (Eds.), 2015, Switzerland, pp. 19-35.

AlDairi Anwaar, Lo'ai Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies", Procedia Computer Science 109C (2017) 1086–1091.

Schomberg, René von . (2013) A Vision of Responsible Research and Innovation, in Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society

(eds R. Owen, J. Bessant and M. Heintz), John Wiley & Sons, Ltd, Chichester, UK. doi: 10.1002/9781118551424.ch3
Pelle, S. & Reber, B., 2015. Responsible Innovation in the Light of Moral Responsibility. *Journal of Chain and Network Science* 12.

Help Net Security (October 20, 2016). "Smart cities face unique and escalating cyber threats" Retrieved from **https://www.helpnetsecurity.com/2016/10/20/smart-cities-cyber-threats/**

Rambus (2017) "Smart Cities: Threat and Countermeasures", Rambus. Copyright © 2017 Rambus.com. Retrieved from https://www.rambus.com/iot/smart-cities/
Matter. 2011. Hilary Sutcliffe "A report on responsible research and innovation". Retrieved from https://ec.europa.eu/research/science-society/document_library/pdf_06/rri-report-hilary-sutcliffe_en.pdf

Macnaghten, P. and Chilvers, J. (2014) The future of science governance: publics, policies, practices, Environment and Planning C: 32: 530–548.

Reys, Nicolas. 2016. "Smart Cities and Cyber Threats", Control Risks Group Limited 2016.. Retrieved from
https://cdn-prd-com.azureedge.net/-/media/corporate/files/our-thinking/insights/smart-cities-and-cyber-threats/smart-cities-article.pdf?modified=20170710141720

Affliation:

Eda Keskin, M. A.
PhD Student
Supervisor: apl. Prof. Dr. Robert Schnepf
Seminar für Philosophie
Martin Luther Universität Halle-Wittenberg
06099 Halle (Saale)

Contact Information:

Eda Keskin
Große Gosenstr. 24 06114
Halle (Saale)
Tel: 0049 179 9495383
E-Mail: edakeskin83@gmail.com

Biographical Sketch

Eda Keskin is a PhD student in branch of philosophy at Martin Luther Universität Halle-Wittenberg. She majored in environmental engineering and philosophy and received M.A. Degree

in Philosophy from the Middle East Technical University, Ankara. She attended Philipps-Universität Marburg as an ERASMUS exchange student, and taught "Social Ecology" class at Europa Universität Viadrina Frankfurt (Oder). She taught classes together with apl. Prof. Dr. Robert Schnepf (MLU) on the philosophies of Theodor W. Adorno and Martin Heidegger. Her research was funded by DAAD STIBET Research and Teaching Assistantship Program. Her doctorate thesis researches the reconstruction of Martin Heidegger's philosophy and the application of his philosophy for the analysis of modern works of artist Joseph Beuys. Her research interests include aesthetics, phenomenology, environmental philosophy and political philosophy. Her M.A. thesis *The Analysis of Alienation [Entfremdung] in Being and Time: From A Marxist Perspective* was published by LAP LAMBERT Academic Publishing on 10. Oktober 2011. Her articles and reviews were published in *Springer*, *Global Justice: Theory Practice Rhetoric, MAHB Stanford University,*
RH+ Art, Cogito, Doğu Batı, Politez, Lacivert, *Nikbinlik*, *Ekin Sanat*, *Ünlem Sanat*, *Patika* and *Dil Im*.