Cybersecurity awareness and education: A necessary parameter for smart communities

Noluxolo Gcaza

CSIR, Meiring Naude Road Brummeria, Pretoria, 0001, South Africa
e-mail: ngcaza@csir.co.za

Abstract

Information and communication technologies (ICTs) are responsible for the transformation of societies, nations and the world at large. ICTs are considered to improve the quality of life for citizens as they bring about easiness and usefulness to perform day-to-day tasks. Most significantly, ICTs have paved way to 'smart' communities whereby citizens integrate various forms of technologies in the different contexts of life. It is known however, that ICTs introduce numerous cybersecurity risks. The problem this paper addresses is that cybersecurity awareness and education in smart communities is not given the precedence it warrants. The paper therefore argues that a community cannot be deemed as 'smart' if it is not 'cyber smart'. As such, the purpose of this paper is to evaluate and highlight the cybersecurity challenges that are prevalent in smart communities.

Keywords

Smart community, ICTs, Cybersecurity awareness and education

1. Introduction

Information and communication technologies (ICTs) remain a constant transformation agent in the everyday life of society in the entire globe. From a global point of view, ICT is seen as a key driver of economic change and innovation. Nationally, ICTs are deemed as a 'catalyst for national integration' (Syed Abdul Kadir, Husin and Nadarajah, 2014). Socially, ICTs are considered to improve the quality of life for citizens in several aspects including how people communicate, play, learn, work, commute, and access health services.

Due to the benefits of ICT, governments nationwide have long committed to employing ICT as a strategy towards human development (Morawczynski, 2007). A study by Kozma and Vota (2014) shows that increased availability and access to ICT improves the quality of life in communities in developing countries. ICTs can facilitate such improvements because they bring about easiness and usefulness to perform day-to-day tasks and access to information (Morawczynski, 2007). Additionally, ICTs improve quality of life by introducing a virtual reality (cyberspace) that eliminates the barriers of time, space, and distance (Rusten and Skerratt, 2007).

ICTs have also paved way to 'smart' living, whereby citizens benefit largely from the innovative ways of doing things (Yan and Shi, 2013). The 'smart' element of living is attributed to the usage of ICTs in the different contexts of life (Lindskog, 2004). ICTs are core to smart living to an extent that one can boldly assert that there can be no smart living without the pervasive integration of ICTs. Smart living is embraced in cities that strive to be more efficient, sustainable and equitable. Inherently such cities are labelled 'smart cities'.

Albino, Berardi, and Dangelico (2015) consider quality of life for citizens as the ultimate aim of a smart city. It is a consent amongst many scholars that "all the smart city initiatives in the end aim to raise quality of life for citizens and other urban stakeholders" (Shapiro, 2006; Batty *et al.*, 2012; Ballas, 2013). Apart from ICTs, the geographic area upon which the city is based, the governing structures and the citizens are the fabric of smart cities (Dameri, 2013). The citizens of a smart city inherently form a smart community. A smart community should ideally comprise of citizens who are self-decisive, independent and aware citizens (Giffinger, 2007). To achieve this, 'smart' initiatives are afforded primarily to transform ordinary communities to smart communities through integration of ICTs amongst other things.

Adversely, it is known that ICTs introduce numerous security risks (i.e. cybersecurity) to its users. However, that cybersecurity awareness and education in smart communities is not given the precedence it warrants. Thus, the purpose of this paper is to analyse the cybersecurity challenges that are prevalent in smart communities. A systematic literature review will be employed as the research method to fulfil this purpose. The paper contents for a smart community that is cyber smart. The sections to follow provide the research an analysis of smart communities. Thereafter, a review of cybersecurity in smart community is provided. Finally, a discussion and concluding remarks can be found.

2. Smart Communities

The inception of the smart communities can be dated back to 1993 in Silicon Valley, California (Lindskog, 2004). This city was among the first to focus on how a community could integrate information technologies towards being 'smart'. Nowadays, the concept of smart communities is used in several contexts. However, a widely accepted definition of a smart community does not exist as yet. This section will explore the concept of smart communities, the elements that make up the community as well as the technologies used in a smart community

2.1 The smart community concept

There are many ideas presented by scholars and domain experts in attempting to define the concept of smart communities. This definitions all have one thing in common – the **use of ICTs**. Some of these definitions are as follows:

- Lindskog (2004) describes a smart community as "a geographical area ranging in size from neighbourhood to a multi-county region whose residents, organizations, and governing institutions are using **information technology** to transform their region in significant ways. Co-operation among government, industry, educators, and the citizenry, instead of individual groups acting in isolation, is preferred. The technological enhancements undertaken as part of this effort should result in fundamental, rather than incremental, changes."

- "The concept of a smart community refers to the use of **information and communication technologies** by local governments and cities to better interact with their citizens, taking advantage of all available data to solve important problems" (Mellouli, Luna-Reyes and Zhang, 2014).

- "A smart community should be defined as a community ranging from a neighbourhood to a nation-wide community of common or shared interest, whose members, organizations and governing institutions are working in partnership to use **information and communication technologies** to transform their circumstances in significant ways" (Albino, Berardi and Dangelico, 2015)

- "A smart community is a community with a vision of the future that involves the application of **information and communication technologies** in a new and innovative way to empower its residents, institutions and regions as a whole. As such, they make the most of the opportunities that new applications afford and broadband-based services can deliver – such as better health care delivery, better education and training, and new business opportunities" (Razak, Malik and Saeed, 2013).

The common component between all the studied definitions can be clearly discerned as the usage of information technologies as means to an end. In addition to the various definitions, there are numerous concepts that are used interchangeably with the term smart community. These include 'community informatics', 'intelligent communities', and 'digital communities' (Albert, 2009). Keenan and Trotter (1990) suggest that community informatics refers to the use of **ICTs** by communities in order to achieve social, economical, political and cultural goals. According to Albert (2009) virtual communities are formed by like-minded people, sharing common interest and are physically separated but virtually united by means of the **Internet**. Intelligent communities are those that view **communication bandwidth** as a necessity for the economic growth and the development of the society. A digital community extends from the intelligent community by combining **communication bandwidth** and innovative services to improve governments, businesses and the lives of the residents of the community (Albert, 2009). Similarly, these synonymous terms reinforce the use of ICTs as the key element of a smart community. Additional elements are discussed in detail in the following subsection.

2.2 The smart community elements

Oksman and Raunio (2018) argue towards smart community elements and suggest the following – smart people, smart governance, smart mobility, and smart living. Firstly, the element of smart people considers participation in public life, the level of education, creativity and flexibility. The level of education factor suggests that "smart people need to be properly educated and trained to operate in the smart city" (Phahlamohlaka *et al.*, 2014). Creativity and flexibility relate to the resourcefulness of the community to leverage from the technological advancements of the city

Secondly, in terms of smart governance, ICT enables citizens engagement, making the community part of the decision making process. Additionally, smart governance aids in addressing democratic issues such as power and inequality in a city (Hollands, 2008). The smart governance component is mostly directed towards promoting intra-city cooperation and community development. Smart governance makes provision for transparent governance by involving citizens' engagement (Castelnovo, Misuraca and Savoldelli, 2016). Essentially, smart governance is related to the manner in which citizens communicate with local government.

Thirdly, smart mobility speaks to local access to sustainable, innovative and safe transportation systems. It emphasizes on convenience, safety and appropriate speed of the transportation systems. Finally, the smart living facet of smart communities focuses on the standard of living for all members of the community i.e. quality of life. The World Health Organization (WHO) defines quality of life as "individuals' perception of their position in life in the context of the culture and value systems" (Whoqol Group, 1995). Quality of life is the general well-being of individuals and societies. In the context of smart communities ITU suggests that quality of life relates to lifestyle in aspects of medical care, welfare, physical safety and education (ITU-T Focus Group on Smart Sustainable Cities, 2014). All the delineated elements are given the smart label because they leverage on the benefits provided by ICTs.

2.3 ICTs in smart community

To this end, it can be clearly perceived that there is a shared assumption on what makes a community smart. The 'smartness' of a community is related to the usage ICTs to achieve the fundamental goals of the community. Moreover, the adaptability of ICTs to be employed in ways that empower and engage the community in political debate contributes to smartness of the community (Hollands, 2008). ICTs that are typically employed in a smart community includes *1) Network Connectivity, 2) Smart Mobile Applications, 3) Sensor Network, 4) Internet of Things (IoTs), 5) Cloud Computing and 6) Big Data Analysis Solutions* (Ezz El-Din, Madhvaraj and Manjaiah, 2016).

Network connectivity enables the community to access available services. In most cases, the community uses these services through smart mobile applications. These services integrate various sensors to continually collect data about the users. Sensors are configured on interconnected devices referred to as Internet of Things (IoTs) that users employ to connect and access services. The data collected from these sensors is commonly stored in the Cloud in order to benefit from convenience of Cloud Computing. Also, the data collected by these technologies is voluminous and is gathered in an exceptionally rapid rate thus the need for Big Data Analysis Solutions.

At the heart of these technologies is the data that is processed and shared by one technology to the other. Smart community technologies processes personally identifiable information (PII) and household level data about citizens (Kitchin, 2016). On one hand, this information can be put to good use by service providers to address service delivery, to enhance the quality of life and to create economic development. On the other hand, the information can be misused by malicious actors thus there is need for cybersecurity efforts.

3. Cybersecurity in smart communities

It is long established that the integration of ICTs in any context introduces the challenge of cybersecurity. As such, cybersecurity is also a challenge in the smart community context. It reported that smart communities are "leading the way towards the adoption of Internet of Things (IoT) technologies that will connect widespread sensors through the cloud to harvest relevant data and automate decision-making processes. Smart cities bring great promise, however there is also risk introduced through this new connectivity and intelligence" (Kaspersky, 2015). Primarily, the adoption of IoTs increases the ways in which an attacker can infiltrate a network i.e. the attack surface (Aldairi and Tawalbeh, 2017). An attack surface is defined as "the total sum of the vulnerabilities in a given computing device or network that are accessible to a hacker" (Rouse, 2014).

A study by Juniper (2018) revealed that IoT botnets could pose an "unmanageable" cybersecurity risk. Botnets are collections of compromised computers which are remotely controlled by an originator with an intention to distribute malicious activities such as distributed denial-of-service (DDoS) attacks, spam and phishing attacks. IoT devices in a smart community can be deployed in Botnet if security requirements are ignored (Wendzel *et al.*, 2014). Kitchin (2016) identifies data privacy and data security as the key challenges that require special attention in smart communities. These challenges are discussed in detail in the following subsections.

3.1 Data privacy

In many nations privacy is extend to citizens as a basic human right to control one's personal information from public scrutiny and unwanted intrusions (Van Der Bank, 2012). Different forms of privacy are outlined as (Martinez-Balleste, Perez-Martinez and Solanas, 2013): *1) Identity privacy* - relating to personal and confidential data. *2) Bodily privacy* - involving the integrity of the physical person. 3*) Territorial privacy* - concerning personal space, objects and property. *4) Locational and movement privacy* – focusing on tracking of one's spatial behaviour. *5) Communications privacy* – concerned with the surveillance of conversations and correspondence. *Transactions privacy* – relating to monitoring of queries/searches, purchases, and other exchanges.

The use of technologies in smart communities exposes the citizens to a wide range of breaches that threaten all the listed forms of privacy (Kitchin, 2016). Smart mobile applications were identified as one of the technologies used in smart communities. These applications are known to raise privacy concerns particularly because they request permissions to device functions to gain access to user information stored in the device (Zang *et al.*, 2015). This information includes but not limited to images, contact details, location information, device information, personal calendars and passwords (Kitchin, 2016).

An additional concern is that the data collected by the smart mobile application can be shared with third parties without the awareness or consent of the user (Kitchin, 2016). Kitchin (2016) adds, the sensors in smart mobile devices collect data that can be analysed and used to infer the health behaviour, social affiliations, sexual orientation as well as lifestyle of users. Essentially, the data collected from these technologies is shared, repurposed and used in unpredictable ways that smart citizens need to be aware of in effort to maintain their privacy.

3.2 Data security

When using ICTs devices the security of information generated, stored, processed and shared is always a concern. It was mentioned that IoTs are prevalent technologies in smart communities. These devices include smartphones, smart locks, smart televisions web cameras to name but a few. These interconnected devices actively participate in processing and exchanging digital information gathered from various sensors (Khoo, 2011). These devices have a number of attack surfaces that open information to a myriad of vulnerabilities (Weber, 2010; Sicari *et al.*, 2015). It is suggested that the security challenges of IoT devices can potentially outweigh the perceived benefits of employing such devices if left unattended (Moganedi and Mtsweni, 2017).

Securing information denotes maintaining the data confidentiality, integrity and availability. According to Moganedi and Mtsweni (2017), when considering security in IoTs, focus needs to be given to data collection, data storage and data communication. Firstly, in terms of data collection, IoT devices collect different types of information that is inclusive of personal information that needs to be secured. A single vulnerability in one of the interconnected IoT device gives a malicious actor an opportunity to manipulate the information thus compromising data integrity. Secondly, the data collected by the IoT device is often stored in the Cloud which introduces another layer of security concerns. Lastly, information communicated in IoT devices is not encrypted due to the lack of sophisticated process capabilities in devices thus information is transmitted insecurely opening a gap for breach of confidentiality.

3.3 Cybersecurity awareness and education

Cybersecurity awareness and education is deemed as a plausible countermeasure and mitigation against cyberattacks to non-technical users such as community members. A study by Wombat Security suggests that cybersecurity awareness is effective for changing behaviour and can reduce the risk of a security breach by up to 70% (Heller, 2015). Moreover, cybersecurity awareness and education is critical in the quest of fostering a positive culture of cybersecurity. Clearly cybersecurity awareness and education has positive impact in minimizing the exposure of home users to cyber-attacks.

The increased attack surface due to pervasive interconnectedness in ICTs is a challenge that citizens of a smart community need to be aware of, thus cybersecurity awareness and education should be acknowledge and pursued as a key parameter in smart communities. This notion is affirmed by findings from a study by Lévy-Bencheton and Barra (2015) which states that cybersecurity awareness and education is lacking necessity in smart communities. Smart citizens include home users that need to be made aware of the related security challenges since smart technologies allow malicious into their home network.

According to Milley (2017), a hacker can access home networks to obtain sensitive information such as banking records. Also, malicious actors can spy on users by hacking into a users' webcam (Jones and Gagneja, 2017). This can potentially place all members of a household at risk. Even worse, smart mobile applications such as digital applications have a complete digital history of users, meaning that if the security is neglected this information can end up in the wrong hands with harmful results to the user (Milley, 2017).

Home users are known to be ill-informed of cybersecurity challenges and thus fall victim to cyberattacks that could have been avoided with minimal security implementations (Thomson, von Solms and Louw, 2006). Awareness and education can provide Internet users with the ability to recognise and circumvent the risks that are apparent online (Kritzinger and Padayachee, 2013).

While the working class may be getting some form of cybersecurity awareness and education from industry, home users and society at large rely on nationally driven cybersecurity awareness and education campaigns (Christensen, 2003). As such, cybersecurity awareness and education has long been recognised as a national priority in many nations. It cannot be disputed that in the modern day, cybersecurity awareness and education is a key requirement in any community that uses ICTs, it is even more critical in a smart community setting as a countermeasure to the increased attack surface.

4. Discussion

It can be gathered from the reviewed literature on smart communities that the ‘smartness’ of a community is inherent to the innovative integration of ICTs in the day-to-day life of citizens. It is also established that these ICTs introduce a vast array of security challenges that necessitate cybersecurity efforts, specifically awareness and education. The high interdependency on ICTs for daily operations the broader the attack surface. Apart from known benefits of ICTs, smart living affords malicious actors the numerous opportunities to infiltrate the network of homes users. Thus cybersecurity awareness and education is a necessity in the context of smart communities.

Accordingly, the previous section highlighted the importance of awareness and education in addressing cybersecurity challenges. Conversely, from smart community literature reviewed there is no mention of cybersecurity awareness and education, which suggests that it is not identified as one of the elements that contribute to the ‘smartness’ of a community. Instead, the emphasis is innovative integration of ICTs in the day-to-day life of citizens, however without cybersecurity awareness and education, these ICTs cannot be used in a secure manner. This paper argues that insecure usage of ICTs cannot be deemed ‘smart’. Thus it is a recommendation that the characterisation of a smart community be re-evaluated to include cybersecurity aware citizenry.

It is imperative to note that these cybersecurity challenges are not unique to smart communities as they affect everyone who uses ICTs. Instead, due to the rapidly increasing attack surface there is a unique urgency to highlight these challenges in the context of smart communities in order to influence the architects and citizens of these communities to accept cybersecurity as a necessary consideration.

Accepting cybersecurity awareness and education as a parameter for smart communities fundamentally means ensuring that each smart city invests in awareness education campaigns for its citizens. Additionally, all role-players in the development of smart cities should be afford cybersecurity measures in all the dimension of smart cities. Finally, it is recommended that the level of cybersecurity should be included as one of the indicators of the ‘smartness’ of a city and respective community.

5. Conclusion

ICTs continuously improve how the world operates on a daily basis. It has lead way to smart communities for the sole purpose of improving the quality of life for citizen. The ‘smart’ label is granted on the basis of using ICTs effectively. These benefits of ICT usage are accompanied by numerous cybersecurity risks that call for cybersecurity awareness and education efforts. This study identified a lack of emphasis on cybersecurity awareness and education in smart community literature. Thus contended towards cyber smart cyber citizens.

6. References

Albert, S. (2009) “Networked Communities: Strategies for Digital Collaboration: Strategies for Digital Collaboration”, IGI Global, United Kingdom, ISBN: 978-1-59904-771-3

Albino, V., Berardi, U. and Dangelico, R. M. (2015) “Smart cities: Definitions, dimensions, performance, and initiatives”, *Journal of Urban Technology,* 22(1), pp. 3–21.

Aldairi, A. and Tawalbeh, L. (2017) “Cyber Security Attacks on Smart Cities and Associated Mobile Technologies”, *Procedia Computer Science*. Elsevier B.V., 109(2016), pp. 1086–1091.

Ballas, D. (2013) “What makes a “happy city”?”, *Cities,* 32(2013), pp. 39–50.

Van Der Bank, C. M. (2012) “The Right To Privacy – South African and Comparative Perspectives”, *European Journal of Business and Social Sciences,* 1(6), pp. 77–86.

Batty, M. et al. (2012) “Smart cities of the future”, *European Physical Journal: Special Topics,* 214(1), pp. 481–518.

Castelnovo, W., Misuraca, G. and Savoldelli, A. (2016) “Smart Cities Governance: The Need for a Holistic Approach to Assessing Urban Participatory Policy Making”, *Social Science Computer Review,* 34(6), pp. 724–739.

Christensen, J. (2003) “Solving the Cyber Security Problem : The Role of the Department of Homeland Security”. Washington, D.C.

Dameri, R. P. (2013) “Searching for Smart City definition: a comprehensive proposal*”, International Journal of Computers & Technology,* 11(5), pp. 2544–2551.

Ezz El-Din, H., Madhvaraj, M. and Manjaiah, D. (2016) “Cyber Security in Smart Cities”, *CSI Communications,* 40(3), pp. 34–36.

Giffinger, R. (2007) “Smart cities - Ranking of European medium-sized cities”, http://www.smart-cities.eu/download/smart_cities_final_report.pdf, (Accessed: 10 June 2018)

Heller, M. (2015) “Cybersecurity awareness can reduce infection risk up to 70%”, News, January, https://www.wombatsecurity.com/news/cybersecurity-awareness-can-reduce-infection-risk-70 (Accesses: 20 July 2018).

Hollands, R. G. (2008) “Will the real smart city please stand up?”, *City*, 12(3), pp. 303–320.

ITU-T Focus Group on Smart Sustainable Cities (2014) “Smart sustainable cities: An analysis of definitions”, https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/.../TR-Definitions.docx (Accessed: 10 June 2018)

Jones, A. S. and Gagneja, K. (2017) “Preventing Covert Webcam Hacking in the Civilian and Governmental Sectors”, *Proceedings - 2016 International Conference on Computational Science and Computational Intelligence,* CSCI 2016, pp. 993–998.

Kaspersky (2015) “Securing Smart Cities Issues Guidelines for Smart City Technology Adoption, Seuring Smart Cities”, https://www.kaspersky.com/about/press-releases/2015_securing-smart-cities-issues-guidelines-for-smart-city-technology-adoption (Accessed: 10 June 2018).

Keenan, T. P. and Mitchell Trotter, D. (1990) “The changing role of community networks in providing citizen access to the Internet”, *Internet Research,* 9(2), pp. 100–108.

Khoo, B. (2011) “RFID As an enabler of the internet of things: Issues of security and privacy”, *in Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing,* iThings/CPSCom 2011, pp. 709–712.

Kitchin, R. (2016) “Getting smarter about smart cities: Improving data privacy and data security”, *Department of the Taoiseach on behalf of the Government Data Forum*.

Kozma, R. B. and Vota, W. S. (2014) “ICT in developing countries: Policies, implementation, and impact”. New York: Springer. ISBN: 978-1-4614-3184-8

Kritzinger, E. and Padayachee, K. (2013) “Engendering an e-safety awareness culture within the South African context”, *in AFRICON. IEEE,* pp. 839 – 843.

Lévy-Bencheton, C. and Darra, E. (2015) “Cyber security for Smart Cities: An architecture model for public transport”.

Lindskog, H. (2004) “Smart communities initiatives”, *Proceedings of the 3rd ISOneWorld Conference,* p. 16.

Martinez-Balleste, A., Perez-Martinez, P. and Solanas, A. (2013) “The pursuit of citizens’ privacy: A privacy-aware smart city is possible”, *IEEE Communications Magazine,* 51(6), pp. 136–141.

Mellouli, S., Luna-Reyes, L. F. and Zhang, J. (2014) “Smart government, citizen participation and open data”, *Information Polity,* 19(1–2), pp. 1–4.

Milley, P. (2017) Privacy and the Internet of Things, Securing the Home IoT Network.

Moganedi, S. and Mtsweni, J. (2017) “Beyond the convenience of the internet of things: Security and privacy concerns”, *in 2017 IST-Africa Week Conference (IST-Africa),* pp. 1–10.

Morawczynski, O. (2007) “Unraveling the impact of investments in ICT, education and health on development: an analysis of archival data of five West African countries using regression splines”, *The Electronic Journal of Information Systems in Developing Countries,* 29(1), pp. 1–15.

Oksman, V. and Raunio, M. (2018) “Citizen -centric Smart City Planning for Africa: A Qualitative Case Study of Early Stage Co-creation of a Namibian Smart Community”, *in The Twelfth International Conference on Digital Society and eGovernments*, pp. 30–35.

Phahlamohlaka, J. et al. (2014) “Towards a Smart Community Centre: SEIDET Digital Village”, *IFIP Advances in Information and Communication Technology*, 431(2009), pp. 107–121.

Razak, N. A., Malik, J. A. and Saeed, M. (2013) “A Development of Smart Village Implementation Plan for Agriculture: A Pioneer Project in Malaysia”, *in Computing & Informatics, 4Th International Conference*, Malaysia, pp. 495–502.

Rouse, M. (2014) “Network Security”, https://whatis.techtarget.com/definition/attack-surface (Accessed: 22 July 2018).

Rusten, G. and Skerratt, S. (2007) “Information and communication technologies in rural society”. Routledge. ISBN: 9781134220823

Shapiro, J. (2006) “Smart cities: quality of life, productivity, and the growth effects of human capital”, *The review of economics and statistics*, 88 (May)(2), pp. 324–335.

Sicari, S. et al. (2015) “Security, privacy and trust in Internet of things: The road ahead”, *Computer Networks*, 76(January), pp. 146–164.

Sorrell, S. (2018) “Internet of Things for Security Providers: Opportunities, Strategies & Market Leaders 2016-2021”, https://www.juniperresearch.com/researchstore/iot-m2m/internet-of-things-for-security-providers/opportunities-strategies-forecasts-(1) (Accessed: 20 July 2018).

Syed Abdul Kadir, S. L., Husin, S. and Nadarajah, D. (2014) “The Impact of ICT on Quality of Life”, *in Advances in Business-Related Research Conference*. Milan, p. 13. http://eprints.um.edu.my/13400/ (Accessed: 20 July 2018).

Thomson, K.-L., von Solms, R. and Louw, L. (2006) “Cultivating an organizational information security culture”, *Computer Fraud & Security*, 2006(10), pp. 7–11.

Weber, R. H. (2010) “Internet of Things - New security and privacy challenges”, *Computer Law and Security Review*. 26(1), pp. 23–30.

Wendzel, S. et al. (2014) “Envisioning smart building botnets”, *in Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI),* pp. 319–329.

Whoqol Group (1995) “The World Health Organization Quality of Life assessment (WHOQOL): position paper from the World Health Organization.”, *Social science & medicine*, 41(10), pp. 1403–1409.

Yan, M. and Shi, H. (2013) “Smart Living Using Bluetooth-Based Android Smartphone”, *International Journal of Wireless & Mobile Networks*, 5(1), pp. 65–72.

Zang, J. et al. (2015) “Who Knows What about Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps”, *Technology Science*. https://techscience.org/a/2015103001/download.pdf (Accessed: 10 June 2018).