Smart Cities at Risk!: Privacy and Security Borderlines from Social Networking in Cities

Vaia Moustaka
Aristotle University of Thessaloniki
+30-2310991865
Greece
vmoustag@csd.auth.gr

Zenonas Theodosiou
SignalGeneriX Ltd.
+357-25870072
Cyprus
z.theodosiou@signalgenerix.com

Athena Vakali
Aristotle University of Thessaloniki
+30-2310998415
Greece
avakali@csd.auth.gr

Anastasis Kounoudes
SignalGeneriX Ltd
+357-25870072
Cyprus
tasos@signalgenerix.com

ABSTRACT

As smart cities infrastructures mature, data becomes a valuable asset which can radically improve city services and tools. Registration, acquisition and utilization of data, which will be transformed into smart services, are becoming more necessary than ever. Online social networks with their enormous momentum are one of the main sources of urban data offering heterogeneous real-time data at a minimal cost. However, various types of attacks often appear on them, which risk users' privacy and affect their online trust. The purpose of this article is to investigate how risks on online social networks affect smart cities and study the differences between privacy and security threats with regard to smart people and smart living dimensions.

CCS CONCEPTS

• **Security and privacy** → Human and societal aspects of security and privacy • **Human-centered computing** → C**ollaborative and social computing**; *Collaborative and social computing systems and tools*; Social Networking Sites

KEYWORDS

smart cities; smart people; smart living; online social networks; privacy threats; security threats

ACM Reference format:
V. Moustaka, Z. Theodosiou, A. Vakali, A. Kounoudes. 2018. Smart cities at risk! : privacy and security threats borderlines from social networking in cities. In *the 2018 Web Conference Companion (WWW' 18 Companion), April 23-27, 2018, Lyon, France*, ACM, New York, NY, 6 pages. DOI: https://doi.org/10.1145/3184558.3191516

1 INTRODUCTION

In recent years, more and more big cities, due to their fragility and the demographic, environmental, economic and financial pressures are taking [1], are striving to acquire the profile of so-called *smart city* and provide smart services to their stakeholders (e.g., citizens, visitors, investors, etc.) [2, 3].

The vision of smart cities (SC), appeared in literature in late 1990s, is a multidisciplinary topic of research since attracts scientists from different research fields (engineering, data science, human science, economics), industries driven from information and communication technologies (ICT) (e.g., CISCO[1], IBM[2], Libelium[3]), governments and policy makers (e.g., EU smart cities initiative[4], Smart City Business Institute[5]), who are cooperating to co-create the cities of tomorrow [4].

SC behave as "living organisms" that evolve over time, and constantly produce and consume heterogeneous data [5]. A huge variety of fixed or moving devices (e.g. sensors, cameras, meters, actuators, RFIDs), the so-called Internet of Things (IoT), and applications (e.g., online social networks (OSN), web platforms, mobile applications, etc.) act as data sources, which record every aspect of city life and produce large-scale heterogeneous data [4]. The penetration of smartphones has facilitated the rapid spread and increase the use of OSN, the users of which are estimated to have reached 2.46 billion in 2017 [6]. The existence of interconnected objects and the exploitation of OSN content result in real-time production of a significantly huge volume of urban data offering limitless opportunities for acquiring profound knowledge of cities and decision-making [4], [7]. In contrast, the excessive zeal and effort to record and monitor any activity within cities raise multiple concerns about the security and privacy of citizens [8]. Critics argue that the implementation of SC will have negative implications on individuals' freedom and privacy as they trade the convenience offered by smart services with the provision of sensitive and personal information [9].

Since civic engagement in the formulation of SC is vital, several researchers addressed the issue of investigating and ensuring privacy and security in the SC context in order to reduce individuals' concerns and suspicion, and empower their participation in social life and cities' efficient operation [15], [33, 34]. The majority of them focused on investigating and addressing cyber-security and privacy-related issues related to ICT infrastructures (e.g., IoT, networks, databases, etc.) and SC applications [8], [10-15]. Specifically, Bartoli et al. [10], summarizing the privacy key issues and emerging technology

WWW '18 Companion April 23-27, 2018, Lyon, France.

ACM ISBN 978-1-4503-5640-4/18/04.
DOI: https://doi.org/10.1145/3184558.3191516

[1] http://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities.html
[2] http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/
[3] http://www.libelium.com/libeliumworld/smart_cities/
[4] http://ec.europa.eu/eip/smartcities/
[5] http://www.smartcbi.org/

standards, highlighted the need to impose high security requirements on IoT technologies used in SC to avoid third-party abuse, and the dissociation between urban and personal data. Furthermore, Beltran et al. [11] have developed the IoT-Architecture Reference Model (IoT-ARM) and its app to empower citizens to use their IoT and feel secure that their privacy is protected. A two-level privacy architecture was also proposed by Mazhelis et al. [13] aiming at protecting the sensitive personal information that citizens disclosure when using various smart applications, while Solomon et al. [14] conducted a comparative assessment of three encrypted-based techniques regarding to smartphone applications that offer close proximity detection preventing any location information leak.

Beyond the risks threaten infrastructure and applications, major privacy and security concerns arise from the underlying risks on OSN. OSN, which are inexpensive tools for data collection and pattern extraction in SC, suffer from various threats and attacks [23] that endanger their users and affect their usefulness and credibility. Unlike the IoT and smart applications, the privacy and security issues arising from their use in SC have not been adequately discussed. Balleste et al. [12] attempted to define citizens' privacy by proposing the "5D privacy model in SC", which concerns all urban data sources used in SC. Of particular interest is also the "2x2 privacy protection framework" proposed by Zoonen, [15] which involves, among others (e.g. IoT, apps, etc.), privacy concerns on OSN, aiming to help policymakers understand and review issues related to the protection of privacy in SC.

Considering OSN as a valuable data source for gaining insight into cities, this article aims to shed light on privacy and security issues related to the OSN use in SC. Exploiting the existing literature, the borderlines between privacy, which depends on individual's perception and attitude, and security, which reflects the quality of life in cities, are set, and their interaction is investigated. Initially, the usefulness of OSN in SC is highlighted, and the potential privacy and security risks appeared on them are presented. Particular emphasis is placed on threats targeted at children since are a sensitive age group of smart people, which will play a significant role in the future of SC. Then, smart people and smart living dimensions are analyzed and their interaction regarding privacy and security issues on OSN is discussed. Finally, a novel relationship model which specifies the relationships between privacy and security threats, along with some useful tools to protect and enhance social networking, is proposed, aiming to address the challenges of privacy and security of OSN in SC.

The contribution of this study is twofold: i) deals with the impact of OSN privacy and security risks on the social dimensions of SC (i.e., smart people and smart living) and attempts to investigate their interaction, and ii) introduces the issue of children' privacy and security protection in SC. Furthermore, the proposed relationship model of security and privacy threats, can be a useful tool for stakeholders who utilize OSN as urban data source and care about individuals' security and engagement in SC.

The rest of this paper is organized as follows: *Section 2* deals with OSN as a source of urban data which are exposed to potential privacy and security risks. *Section 3* identifies the main characteristics of smart people and smart living dimensions and discusses their interaction on privacy and security issues on OSN. *Section 4* proposes the relationship model of privacy and security threats and suggests some useful tools to protect and encourage the participation of people on OSN. Finally, *Section 5* contains some conclusions and future perspectives.

2 OSN IN SMART CITIES: OPPORTUNITIES & THREATS

The proliferation of OSN, which are used mainly as means of interactive communication among individuals, offers new possibilities for recording and analyzing data about human activities and the cities in which they live. However, OSN, sometimes, because of their misuse, prove dangerous for the privacy and security of individuals and cities, respectively. The opportunities and threats that arise from their use are analyzed in the following subsections.

2.1 OSN as Urban Data Source

OSN (e.g. Facebook, Twitter, Foursquare, Instagram, etc.) acting as "human sensors", compared to IoT, offer volumes of heterogeneous data, reduced costs, interoperability, and dependability [16]. Examining the impact of OSN on e-government and e-participation, Dameri and Ricciardi [17], concluded that OSN can make a significant contribution to: i) service delivery, ii) governance participation, and iii) smartness awareness. Doran et al. [16], using geo-located data from Twitter, have recognized and visualized various geographic, social, cultural and political characteristics that have led to the extraction of citizens' perceptual patterns in a large city, while Kumar & Ahmed [18] exploited Twitter for traffic event detection. OSN, due to their advantages, have already been widely utilized for the implementation of SC either independently or complementary to the IoT and their use is expected to increase in the future [4], [16], [12-14].

2.2 Threats & Privacy Risks

Despite the fact that OSN is a useful tool for stakeholders (e.g., local authorities, companies, etc.) that exploit the data produced, many privacy and security concerns arise. Individuals increasingly register and share personal information (such as date of birth, email address, telephone number, home address, photos, videos, etc.) on OSN and their content can be used in many ways exposing them to danger. In many cases human activity, sentiment and opinion of individuals on OSN are recorded and analyzed in their absence [12], [19, 20].

For the purpose of investigating the privacy and security concerns raised in the SC context, at this point, we will clarify the terms of "privacy" and "security", which are often confused. *Privacy* concerns the protection of individual's personal information from the illegal disclosure and use by third malicious parties and is directly related to the individual's online behavior and privacy preferences [12], [21, 22]. Individuals' belief that their privacy is more protected than that of others, and the degree of their trust in other users compromise their privacy [35, 36].

According to Zhang et al. [21] individual's privacy on OSN consists of:

1. *Individual's identity anonymity:* concerns the protection of the user's identity, so that it is not easily detected on the Internet.
2. *Individual's personal space privacy:* refers to access control to a user's profile, in particular information and content posted on it.
3. *Individual's communication privacy:* concerns the protection of information related to the connection network (e.g., IP address, location etc.) and the user's navigation activities (e.g., friends, messages sent etc., online preferences etc.).

On the other hand, *security* refers to the protection of OSN users from threats caused either by inside attackers (i.e. other OSN users) or by external attackers (i.e., individuals who do not participate but can commit attacks on the OSN system) who exploit the unawareness and naivety of their potential victims [21].

Many research efforts have focused on identifying and dealing with risks and threats affecting OSN [21-23]. According to Fire et al. [23], OSN threats can be divided into the following four main categories, the subcategories of which are depicted in Fig. 1.

1. *Classic threats:* threats that occurred when the Internet was created and spread, and referred as malware, phishing, spam or cross-site scripting attacks. Although these threats have been addressed in the past, due to the spread of OSN, they are becoming more viral and spreading through their users and their friends.
2. *Modern threats:* threats related to OSN and target the individuals' personal information and the personal information of their friends. Information and location leakage, fake profiles, identity clone attacks and face recognition are just some of these threats.
3. *Combination threats:* threats which are the combination of classic and modern threats to create more effective threats.
4. *Threats targeting children:* threats directed exclusively at children and adolescents. Online predators, cyber-bullying and children's risky behaviors when communicate online with strangers and publish private information and photos on OSN are the most risky of these threats.

OSN users are also exposed to risks by their share multimedia content, many of which are indirect or often ignored by the majority of them. The most dangerous from these risks are: *i) multimedia content, ii) lack of policies, iii) platform vulnerabilities and iv) open access.* The individual's sensitive and personal content is stored, daily, as multimedia files on OSN, which are software platforms vulnerable to the bugs and malicious third parties. Additionally, the lack of policies to govern every possible privacy issue or to allow fine-grained user customization and the existing "freemium" model, which allows individuals to register quite easily, contribute to the creation of multiple and false accounts complicating the detection of malicious actors [22].

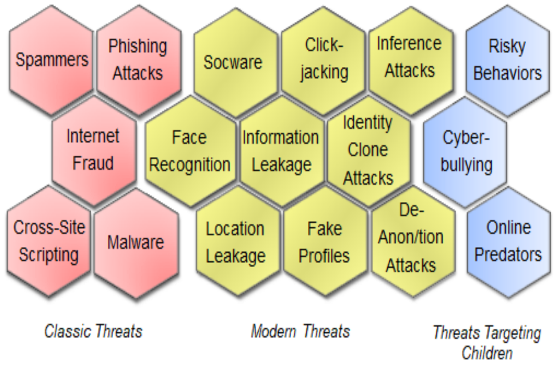

Figure 1: Threats on OSN

The most peculiar and dangerous threats mentioned above are threats targeting children. These threats, which can be extended to adults, are usually caused by psychological factors and occur both in real life and in online life. Online predators and cyber-bullying attacks are booming nowadays. Adults or minors in order to satisfy their fantasies and to erase their frustration and anger, often, sexually harass or intimidate their potential victims [23]. Parents cannot fully protect their children whose critical ability and online defense on OSN are minimal, while in many cases adults are sharing sensitive personal information and photos on OSN regarding to their children, exposing them to privacy and security risks [24]. The Canadian Centre for Child Protection[6] has revealed that children under 12 years old were depicted in 78.30% of the images and videos assessed by their team. Furthermore, recent surveys have revealed that cyber-bullying[7] occurs mainly through OSN, while more than 82% of online sex crimes related to sexual predators[8] and online sexual offenses originate from OSN that predators use to gain insight into their victims. As these threats greatly affect children's behavior and psychology, they can have disastrous and irreversible effects, such as in the cases of Amanda Michelle Todd and Rebecca Ann Sedwick, both of whom committed suicide after being cyber-bullied on Facebook [23, 24].

3 SMART CITIES DIMENSIONS RISKS

The conceptual model of Giffinger & Gudrun [25], which is widely accepted in bibliography [2-5], recognize that SC consist of six dimensions*: i) smart mobility, ii) smart economy, iii) smart environment, iv) smart governance, smart people and iv) smart living*. Since OSN directed and used by people and influence social life and safety of people, in this article, we focus on *smart people* and *smart living* dimensions which are related to the social perspective of SC [2].

3.1 Smart People

People are recognized by many researchers as the main pillar of SC since ICT and other SC infrastructures without human

[6] https://www.protectchildren.ca/app/en/
[7] http://enough.org/stats_cyberbullying
[8] http://www.kidslivesafe.com/child-safety/online-predators-and-cyberbullying-statistics

intervention become inadequate [2], [4], [25, 26]. The main characteristics of smart people are summarized in: i) *human factors*, which are *creativity, social learning and education*, and ii) *social factors*, such as *social ethnic plurality, open-mindedness and individuals' participation in public life* [2], [26]. Individuals share their opinions, feelings and content on OSN, record data through personal IoT (e.g. wearable devices, smart meters in their homes, personal health applications etc.), and in some cases participate in surveys and crowdsourcing activities (e.g, SEN2SOC[9] platform, etc.) [4]. Their data is an asset to cities as offers knowledge and helps in decision-making.

With regard to OSN, when individuals combine some or all of the aforementioned smart factors and provide, knowingly and responsibly, their personal data, taking into account all privacy and security threats, can contribute significantly to preservation and improvement of security in cities. Privacy is primarily personal responsibility, is ensured by the proper use of the proposed privacy settings and can lead to security protection as individuals cease to be vulnerable to malicious parties. Recent studies revealed that the only way to enhance the involvement of individuals is to feel safe that their personal data recorded by the various devices and applications are fully protected and that they control the purpose of its use [13]. Thus, the feeling of security and confidence on OSN, will enhance the participation of individuals, which in collaboration with their fellow citizens and local authorities will co-create new smart services and strengthen social cohesion [15], [27].

On the contrary, the lack of skills, education and awareness of individuals about the safe use of the OSN leads them to naivety, carelessness and loss of control making them vulnerable to the underlying privacy and security risks [23]. Therefore, malicious actors have the opportunity to attack and achieve their goals, degrading security on OSN and causing concerns and fears for their users. Concerns about the leakage of privacy and the purpose of using data collected by third parties discourage the individuals' involvement on OSN and social life, leading to the registration of inaccurate and false data that affects adversely SC [15], [28]. Thus, individuals' "smartness" decreases.

3.2 Smart Living

Despite that smart living is one of the most discussed dimensions and is indissolubly associated with people since it determines the level of urban services provided and well-being in cities. This dimension involves services that cover almost all human needs, such as transport, health, public safety and security, culture, entertainment, education, entrepreneurship, etc., [2], [4], [25].

The breadth of smart living requires the understanding of needs and the development of smart services, as well as their monitoring and improvement [2-5], [25]. As the data, which is generated from all available data sources, is circulated at a fast pace, new privacy and security issues arise, which have dual impact on smart living: on the one hand, the risks associated with attacks on SC infrastructures (e.g., databases, IoT networks, applications, etc.) [8-14] and OSN are particularly detrimental to public security and the individuals' privacy, as outlined in Section 2; on the other hand individuals, influenced by common privacy and security threats on OSN, lose their online trust and become unwilling to participate in the development of smart services [15].

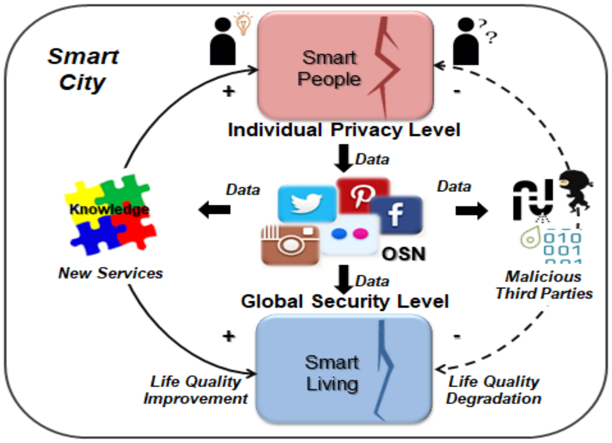

Figure 2: "Privacy VS Security" in smart cities

3.3 Individual Privacy VS Global Security

As evidenced by the aforementioned, there is a strong interaction and correlation between the individuals' privacy perception and the public perception of security in cities, which affect significantly smart people and smart living dimensions. Privacy protection at individual privacy level can drive to global security level in cities and vice-versa, as depicted in Fig 2. The degree of influence of human and social factors on individuals determines their behavior and attitudes towards data provision and privacy issues and has a positive or negative impact on security in cities. Specifically, as shown in Fig. 2, when individuals use OSN wisely, taking care to protect their privacy, contribute to achieving security in cities and by extension to the improvement of life quality. Additionally, social networking data is transformed into valuable knowledge for cities, leading to the development of new services and the enhancement of smart living. Otherwise, individuals put their privacy at risk and facilitate the work of malicious third parties, causing public concerns and decreasing security in cities.

On the other hand, in the closed system of SC, individuals' attitudes and perceptions of privacy are influenced by the prevailing public perceptions and the level of security and life quality in the cities. Individuals often lose their online trust, due to common concerns and fears about the leakage and misuse of their personal data by dangerous third parties, as depicted in Fig 2. Mistrust and suspicion towards OSN discourage the participation of individuals on them and favor the entry of untrue data, affecting adversely individuals' engagement in SC and decreasing their "smartness". The proper information and awareness policy of individuals by local authorities, as Zoonen [15] pointed out, as well as the development and dissemination of useful tools that protect individuals' privacy, can drive to smart behavior and

[9] http://smartsantander.eu/index.php/sen2soc

empower individuals' active participation in formulation of smart living.

4 PRIVACY AND SECURITY CHALLENGES IN SMART CITIES

Since the contribution of OSN is especially beneficial for SC, particular attention should be paid to tackling the privacy and security challenges that affect smart people and smart living. For this purpose, we distinguish two main steps which are analyzed in the following subsections. The first step concerns the understanding of differences between privacy and security threats to identify vulnerabilities that facilitate abusers, and the second step concerns taking the necessary countermeasures (e.g., legislation, tools, etc.) to prevent and deal with them.

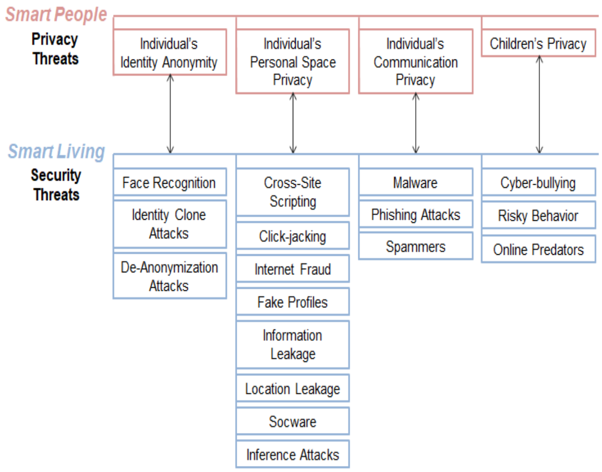

Figure 3: Relationships between Privacy and Security threats

4.1 Privacy VS Security Threats

The exploitation of existing literature [21-24] related to privacy and security threats on OSN in conjunction with the identification of the interaction of smart people and smart living regarding privacy and security in SC (discussed in Section 3), has led us to understand the differences between privacy and security threats and define the borderlines between them (Fig. 3). As demonstrated in Fig. 3, individuals' privacy on OSN is threatened by risks associated with their identity, profile content, and communication network information [21]. Moreover, risks that threaten children's privacy, which are a special case, have been also added. The security threats [23] caused by third parties and degrade the life quality in cities, were analyzed and their relations with the aforementioned privacy threats were defined. The proposed relationship model of privacy and security threats is based on the analysis of the security attacks, presented by Fire et al. [23], and how these attacks are correlated with the privacy threats [21] presented in subsection 2.2.

The proposed model that specifies the relationships between the potential privacy and security threats on OSN can be a useful tool for stakeholders who utilize OSN as urban data source and care about individuals' security and engagement in SC. For instance, they can develop novel smart and specialized tools and applications to protect or educate individuals and children on OSN, contributing to both smart people (e.g., education, awareness, engagement etc.) and smart living (e.g., privacy and security protection etc.).

4.2 Problem Resolving

Dealing with privacy and security threats depends mainly on individuals' personal background (e.g., maturity, experiences, education, skills, psychology, awareness, etc.). However, the excessive exposure of individuals, and in particular children, to ICT and OSN, the lack of adequate and revised legislation and the failure of OSN to protect effectively their users, increase the privacy and security risks and attacks in cities [21-24], [29, 30].

Beyond training, education and appropriate awareness, a variety of methods and tools has been proposed and developed aiming at increasing the protection of privacy on OSN and "awakening" individuals [22], [30]. Fire et al. [23] in their work discussed OSN operator, commercial and academic solutions (e.g., OSN privacy & security settings, MinorMonitor, Defensio, socware detection, phishing detection, etc.), while Patsakis et al. [22] presented possible solutions for the protection of multimedia content on OSN (e.g., watermarking, steganalysis, storage encryption, etc.).

With regard to threats targeting children, despite their complexity, effective tools have been developed. Various add-ons have been developed to help parents block pornographic or inappropriate content (e.g. FoxFilter[10]), and empower individuals to protect their photos online (e.g., Cryptagram) [31]. A new browser-based architecture that aims to protect minors, and not just, from malicious attacks on OSN is also designed and developed in the framework of the ENCASE Project[11]. The proposed user-centric architecture leverages the latest advances in usable security and privacy aiming to form an effective protective net against cyber-bullying and sexually abusive [32].

5 CONCLUSIONS

This article investigates the security and privacy issues of OSN in the SC context. The analysis has demonstrated that there is a strong interaction and correlation between individual's privacy perception and public perception of security. Privacy protection at individual privacy level (smart people) can drive to global security level (smart living), and vice–versa. The differences between privacy and security threats were studied and their borderlines were defined. The proposed relationship model of privacy and security threats, can enable stakeholders to understand the needs in the use of OSN and develop the appropriate tools for enhancing the privacy and security in smart cities.

Education and cultivation of prudent and safe behavior on the Internet and OSN combined with the methods and tools developed to protect against privacy and security risks on OSN can make a decisive contribution to shaping smart people and enhancing the

[10] https://addons.mozilla.org/en-us/firefox/addon/foxfilter/
[11] http://encase.socialcomputing.eu/

quality of life. Active citizens, interested in the cities they live in, will be able to use properly the OSN to offer valuable urban information without worrying about their online security. With regard to smart living, the benefit will be twofold as citizens' privacy and security will be enhanced and the exploitation of data derived from OSN will lead to the improvement and development of new smart services.

In the future, we plan to expand our work by studying smart peoples' behavior when dealing with privacy threats and security risks on OSN, with the aim of identifying and addressing vulnerabilities in order to enhance their significant involvement in SC through social networking.

ACKNOWLEDGMENTS

Authors acknowledge research funding from the European Union Horizon 2020 research and innovation programme under the Marie Skodowska-Curie grant agreement No 691025.

REFERENCES

[1] NOKIA, Machina Research Smart City Playbook. 2016. https://pages.nokia.com/2170.What.Are.Cities.Doing.to.Be.Smart.html

[2] M. Batty, K-W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis and Y. Portugali. 2012. Smart cities of the future. *The European Physical Journal Special Topics* 214, 1 (Nov. 2012), 481-518. DOI: http://dx.doi.org/10.1140/epjst/e2012-01703-3

[3] L.-G. Anthopoulos. 2017. *Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick?.* Springer International Publishing. DOI: 10.1007/978-3-319-57015-0

[4] V. Moustaka, A. Vakali, and L.-G. Anthopoulos. 2018. A systematic review for smart city data analytics (under review)

[5] V. Moustaka, A. Vakali, and L.-G. Anthopoulos. 2017. CityDNA: smart city dimensions' correlations for identifying urban profile. In *Proceedings of the 26th International World Wide Web Conference (WWW2017)*, ACM. DOI: https://doi.org/10.1145/3041021.3054714

[6] Statista. 2018. Number of social media users worldwide from 2010 to 2021 (in billions). Retrieved, Jan. 2018, from: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

[7] E.-A. Nuaimi, H.-A. Neyadi, N. Mohamed, and J. Al-Jaroodi. 2015. Applications of big data to smart cities. *Journal of Internet Services and Applications* 6, 25. DOI 10.1186/s13174-015-0041-5

[8] A.-S. Elmaghraby and M.-M. Losavio. 2014. Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research* 5, 491-497. DOI: https://doi.org/10.1016/j.jare.2014.02.006

[9] K.-B. Ahmed, M. Bouhorma, and M.-B. Ahmed. 2014. Age of Big Data and Smart Cities: Privacy TradeOff. *International Journal of Engineering Trends and Technology (IJETT)* 16, 6 (Oct 2014). Retrieved, Dec. 2017, from: https://arxiv.org/ftp/arxiv/papers/1411/1411.0087.pdf

[10] A. Bartoli, J. Hernandez-Serrano, M. Sorian, M. Dohler, A. Kountouris, and D. Barthel. 2011. Security and Privacy in your Smart City. In *Proceedings of Barcelona Smart Cities Congress.* Retrieved, Dec. 2017, from: http://www.cttc.es/publication/security-and-privacy-in-your-smart-city/

[11] V. Beltran, A. F. Skarmeta, and P.-M. Ruiz. 2017. An ARM-Compliant Architecture for User Privacy in Smart Cities: SMARTIE—Quality by Design in the IoT. *Wireless Communications and Mobile Computing.* DOI: https://doi.org/10.1155/2017/3859836

[12] A. Martínez-Balleste, P.-A. Pérez-Martínez, and A. Solanas. 2013. The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *IEEE Communications Magazine* 51, 6 (June 2013), 136-141. DOI: http://dx.doi.org/10.1109/MCOM.2013.6525606

[13] O. Mazhelis, A. Hämäläinen, T. Asp. and P. Tyrväinen. 2016. Towards enabling privacy preserving smart city apps. In *Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2),* IEEE. DOI: 10.1109/ISC2.2016.7580755

[14] M.-G. Solomon, V. Sunderam, L. Xiong, and M. Li. 2016. Enabling mutually private location proximity services in smart cities: A comparative assessment. In *Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2),* IEEE. DOI: 10.1109/ISC2.2016.7580757

[15] L. Van Zoonen. 2016. Privacy concerns in smart cities. *Government Information Quarterly* 33, 3 (July 2016), 472-480. DOI: https://doi.org/10.1016/j.giq.2016.06.004

[16] D. Doran, K. Severin, S. Gokhale, and A. Dagnino. 2014. Social Media Enabled Human Sensing for Smart Cities. *AI Communications 2014.* Retrieved, Dec. 2017, from: http://knoesis.wright.edu/sites/default/files/aic14.pdf

[17] R.-P. Dameri and F. Ricciardi. 2014. Using Social Networks in Smart City:organizational challenges, synergies, and benefits. In *Proceedings of the European Conference on Social Media (ECSM 2014)*

[18] K.-E. Kumar and H.-A. Ahmed. 2016. Estimation of Traffic with Accuracy through Twitter Stream Analysis. *International Journal of Innovative Technlogies* 04, 08 (July 2016), 1317-1324

[19] G. Rizzo, R. Meo, R.-G. Pensa, G. Falcone, and R. Troncy. 2016. Shaping City Neighborhoods Leveraging Crowd Sensor. *Information Systems*, July 2016. DOI: http://dx.doi.org/10.1016/j.engappai.2012.05.005

[20] F. Luo, G. Cao, K. Mulligan and X. Li. 2016. Explore spatiotemporal and demographic characteristics of human mobility via Twitter: A case study of Chicago. *Applied Geography* 70, May 2016, 11-25. DOI: http://dx.doi.org/10.1016/j.apgeog.2016.03.001

[21] C. Zhang and J. Sun. 2010. Privacy and Security for Online Social Networks: Challenges and Opportunities. *IEEE Network 24,* 4 (July-August 2010). DOI: 10.1109/MNET.2010.5510913

[22] C. Patsakis, A. Zigomitros, A. Papageorgiou and A. Solanas. 2014. Privacy and Security for Multimedia Content shared on OSNs: Issues and Countermeasures, *Computer Journal* 58, 4, 518-535. DOI: https://doi.org/10.1093/comjnl/bxu066

[23] M. Fire, R. Goldschmidt and Y. Elovici. 2014. Online Social Networks: Threats and Solutions, *IEEE Communication Surveys & Tutorials* 16, 4, Fourth Quarter 2014, 2019-2036

[24] T. Minkus, K. Liu, and K.-W. Ross. 2015. Children Seen But Not Heard: When Parents Compromise Children's Online Privacy. In *Proceedings of the 24th International Conference on World Wide Web (WWW'15),* 776-786. DOI: https://doi.org/10.1145/2736277.2741124

[25] R. Giffinger and H. Gudrun. 2010. Smart Cities Ranking: An Effective Instrument for the Positioning of Cities?. *ACE 4,* 12 (February 2010), 7-25, URI=http://hdl.handle.net/2099/8550

[26] T. Nam and T.-A. Pardo. 2011. Conceptualizing 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 (dg.o' 11),* ACM. DOI: https://doi.org/10.1145/2037556.2037602

[27] J. Lee and H. Lee. 2014. Developing and validating a citizen-centric typology for smart city services. *Government Information Quarterly 31,* s93-s105. DOI: https://doi.org/10.1016/j.giq.2014.01.010

[28] B. Kantarci and H.-T. Mouftah. 2014. Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things. *IEEE Internet of Things Journal* 1, 4 (Aug. 2014). DOI: http://dx.doi.org/360-368. 10.1109/JIOT.2014.2337886

[29] R. Shillair, S.-R. Cotton, H.-Y-S. Tsai, S. Alhabash, R. LaRose, and N.-J. Rifon. 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 48, 199-207. DOI: https://doi.org/10.1016/j.chb.2015.01.046

[30] Y. Li, Y Li., Q. Yan, and R.-H. Deng. 2015. Privacy leakage analysis in online social networks. *Computers & Security* 49, 239-254. DOI: https://doi.org/10.1016/j.cose.2014.10.012

[31] M. Tierney, I. Spiro, C. Bregler and L. Subramanian. 2013. Cryptagram: Photo privacy for online social media. In *Proceedings of the 1st ACM Conference on Online Social Networks (COSN'13),* 75-88, ACM, New York, NY, USA.

[32] A. Tsirtsis, N. Tsapatsoulis, M. Stamatelatos, K. Papadamou, and M. Sirivianos. 2016. Cyber Security Risks for Minors: A Taxonomy and a Software Architecture. In *2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP),* IEEE. DOI: https://doi.org/10.1109/SMAP.2016.7753391

[33] L. Van Zoonen & G. Turner. 2013. Taboos and desires of the UK public for identitymanagement in the future: Findings from two survey games. *In Proceedings of the 2013 ACM workshop on Digital Identity Management (DIM '13),* 37-44. DOI: https://doi.org/10.1145/2517881.2517887

[34] T. Kirby. 2014. Controversy surrounds England's new NHS database. *The Lancet* 383, 9918. http://www.thelancet.com/journals/lancet/article/PIIS0140-6736(14)60230-0/fulltext

[35] Y.-M. Baek, E-M Kim, and Y. Bae. 2014. My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns *Computers in Human Behavior* 31, Feb. 2014, 48-56. DOI: https://doi.org/10.1016/j.chb.2013.10.010

[36] A. Bergström. 2015. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior* 53, Dec. 2015, 419-426. DOI: https://doi.org/10.1016/j.chb.2015.07.025