Technological Forecasting & Social Change 142 (2019) 285–300

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

journal homepage: www.elsevier.com/locate/techfore

Enhancing social networking in smart cities: Privacy and security borderlines

Vaia Moustaka[a,*], Zenonas Theodosiou[b], Athena Vakali[a], Anastasis Kounoudes[b], Leonidas G. Anthopoulos[c]

[a] Aristotle University of Thessaloniki, Thessaloniki, Greece
[b] SignalGeneriX Ltd, Limassol, Cyprus
[c] TEI of Thessaly, Larissa, Greece

ARTICLE INFO

Keywords:
Smart people
Smart living
Online social networks
Behavioral patterns
Privacy
Information security
Engagement

ABSTRACT

The proliferation of social platforms and the enhanced connectivity have led people of different age groups, ethnicity, social or economic status to reveal a great deal about themselves online. Data collected from online social networks (OSN) provides social, economic, and cultural information which can be utilized by governments, policy makers, authorities and even commercial industries to better understand market trends and behavioral patterns, that can influence the individual dynamics through open data sources. OSN constitute a breeding ground for the spread of several risks and threats to privacy and security that affect participation and quality of life in smart cities. Although the aspects of privacy and security, and individuals' behavior in social networking are important for the successful development of smart cities, they have not been adequately discussed. To this end, this study aims to address this issue by revealing the risks, threats and individuals' behavior on OSN as an attempt to enhance privacy and security, and boost community's engagement in smart cities. Furthermore, a novel model which outlines the relationships between privacy and security threats, along with some effective countermeasures for the protection of OSN users in smart cities are proposed.

1. Introduction

Demographic, environmental, economic and technological trends in combination with urban sustainability have led to the design and development of *smart cities* (SC), which are expected to be able to address recent and future challenges by taking advantage of Information and Communications Technologies (ICT) (Anthopoulos, 2017; Nokia, 2016). The acquisition of urban knowledge, which comes from the exploitation of urban data, helps cities to identify local weaknesses and opportunities and determines decision-making and smart service deployment, while they concern major prerequisites for transforming a typical city to a SC (Moustaka et al., 2018a; Nuaimi et al., 2015). In this regard, a wide variety of fixed or portable devices (e.g., sensors, cameras, meters, actuators and RFID, etc.), the so-called Internet of Things (IoT), and applications (e.g., OSN, web platforms, mobile applications, etc.) has been developed and utilized to capture different aspects of life in cities (Moustaka et al., 2018a). Recent facts have revealed that 4.9 billion objects became Internet-connected in 2017, while this number is expected to reach or exceed 50 billion in 2020 (Marr, 2017).

In addition, smartphone penetration has led to the rapid expansion and increased use of OSN, the users of which it is estimated that exceeded the population of 2.46 billion in 2017 (Statista, 2018). A huge amount of heterogeneous urban data streams, generated from the aforementioned data sources, result to the transition from “data-informed urbanism” to “data-driven urbanism”, as aptly pointed out by Kitchin (2016).

Whilst data is a valuable asset for cities, its collection and processing methods, ownership regime and the purpose of their use raise serious ethical issues, which must be addressed by the SC stakeholders (e.g., policy makers, researchers, companies and utilities, etc.) (Bianchini and Avila, 2014; Cobb, 2016; Kitchin, 2016). In several cases, the collected data for public benefit was, ultimately, exploited by both public and private organizations for their own purposes (e.g., mass control, market dominance, dataveillance, etc.), violating the privacy rights of individuals and overshadowing the vision of SC (Bianchini and Avila, 2014; Cobb, 2016; Greenfield, 2013; Kitchin, 2014; Kitchin, 2016; Townsend, 2013). Excessive zeal and efforts to record and monitor activities within cities, and vulnerabilities of ICT infrastructures have

* Corresponding author.
E-mail addresses: vmoustag@csd.auth.gr (V. Moustaka), z.theodosiou@signalgenerix.com (Z. Theodosiou), avakali@csd.auth.gr (A. Vakali), tasos@signalgenerix.com (A. Kounoudes), lanthopo@teilar.gr (L.G. Anthopoulos).

https://doi.org/10.1016/j.techfore.2018.10.026
Received 10 May 2018; Received in revised form 30 September 2018; Accepted 29 October 2018
Available online 06 November 2018
0040-1625/

raised numerous security and privacy concerns, and in many cases have annoyed citizens (Elmaghraby and Losavio, 2014; Zoonen, 2016). Critics argue that the implementation of SC will have negative implications on individuals' freedom and privacy as they trade off the convenience offered by smart services with the provision of sensitive and personal information (Ahmed et al., 2014). Hence, these privacy and ethical issues have a negative impact on the involvement of citizens in SC development, as they feel they are constantly being monitored and their fears about privacy and security are emerging (Zoonen, 2016; Kirby, 2014).

Several researchers have dealt with privacy and security issues in SC in order to develop ethical and safe cities that will respect and protect their citizens from malicious attacks and data breaches. (Bianchini and Avila, 2014; Kitchin, 2016; Zoonen, 2016). The majority of them focused on cyber-security and privacy- issues related to ICT infrastructure (e.g., IoT, networks, databases, etc.) and SC applications (Bartoli et al., 2011; Beltran et al., 2017; Elmaghraby and Losavio, 2014; Martinez-Balleste et al., 2013; Mazhelis et al., 2016; Solomon et al., 2016; Zoonen, 2016). Specifically, Bartoli et al. (2011) 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. (2017) have developed the IoT-Architecture Reference Model (IoT-ARM) and its app to empower citizens to use their IoT and feel safe that their privacy is protected. A two-level privacy architecture was also proposed by Mazhelis et al. (2016), which aims to protect sensitive personal information from smart applications, while Solomon et al. (2016) conducted a comparative assessment of three encryption-based techniques regarding smartphone applications that offer close proximity detection preventing any location information leak.

In contrast to infrastructure and applications, research on privacy and security issues related to OSN activities in the SC context is incomplete (Moustaka et al., 2018b). To the best of our knowledge, only a few works deal with the study of privacy and security of OSN in SC. Specifically, Martinez-Balleste et al. (2013) attempted to define citizens' privacy by proposing the "5D privacy model in SC", which concerns all urban data sources used in SC, while Zoonen (2016) has proposed the "2 × 2 privacy protection framework" that involves, among others (e.g., IoT and apps, etc.), privacy concerns on OSN, aiming to help policymakers understand and review issues related to the protection of privacy in SC.

The conceptual model of Giffinger and Gudrun (2010), for instance, analyzes SC in the following six dimensions: *i*) *smart mobility*, *ii*) *smart economy*, *iii*) *smart environment*, *iv*) *smart governance*, *smart people* and *iv*) *smart living* (Anthopoulos, 2017; Batty et al., 2012; Moustaka et al., 2017; Moustaka et al., 2018a). The performance of these dimensions and their sub-dimensions can be evaluated by the Key Performance Indicators (KPIs), which have been introduced by the ITU[1] SC Focus Group and adopted by ISO/TR 37150 (ISO/IEC, 2015; ITU-T FG-SSC, 2014). According to Moustaka et al. (2018a), scholars have focused on smart mobility and IoT, while a few studies have dealt with security issues and individuals' behavior in SC. Taking into account this gap in conjunction with the lack of studies on the secure and constructive use of OSN in SC, as previously discussed, this article aims to shed light on the privacy and security issues related to the OSN use in SC, via investigating behavioral patterns on OSN. These patterns will reveal individuals' vulnerabilities and help *SC stakeholders* (*policy makers*, *local authorities*, *companies*, *researchers*, etc.) designing, adopting and applying the appropriate policies for the cultivation of smart people who will participate responsibly and safely in OSN in SC. More specifically, this article aims to provide with answers the following research questions:

RQ1. What vulnerabilities lie behind individuals' activities in OSN in SC that threaten individuals' privacy and security?

RQ2. What are the individuals' behavioral patterns in OSN that could be exploited by SC stakeholders, with the purpose of adopting and applying the appropriate policies aiming at enhancing protection of individuals during social networking and encouraging their participation in SC?

Both these questions are important to be answered, since more and more SC services are being deployed, which interact and collect data in combination with OSN. Moreover, citizens' ICT literacy concerns a significant SC driver and it is not necessarily at the appropriate level in all SC cases.

In order to answer the above research questions, this article initially highlights the usefulness of OSN in SC, and discusses corresponding potential privacy and security risks. Particular emphasis is given on threats targeted to children who concern a sensitive SC user group, which will play significant role with regard to the future development of SC. Then, smart people and smart living dimensions, which are linked to privacy and security and individual's behavior over OSN, are analyzed and their interaction regarding privacy and security issues on OSN is discussed. The behavioral patterns on OSN are also explored, with the aim of identifying and addressing individuals' vulnerabilities to turn them into smart people who will be actively involved in the implementation of SC. Finally, a novel relationship model which specifies the borderlines between privacy and security threats along with some appropriate measures to protect and enhance social networking are proposed, aiming to cultivate smart people, to address the challenges of privacy and security of OSN in SC, and create safer and more ethical cities. The proposed model is tested and validated by an empirical study which concerns evidence from the SC of Trikala.

The contribution of this article is twofold: i) it studies how privacy and security on OSN interact and affect smart people and smart living dimensions, identifying the borderlines between them, and ii) investigates behavioral patterns of individuals on OSN and discusses some indicative measures, with the aim of transforming them into smart people and enhancing their significant engagement in SC through social networking. Furthermore, the proposed relationship model of security and privacy threats can become a useful tool for SC stakeholders who utilize OSN as urban data source and care about individuals' security and engagement in SC.

The rest of this paper is structured as follows: *Section 2* deals with OSN, which are one of the main sources of urban data, and their potential vulnerabilities that endanger privacy and security of their users. *Section 3* investigates the interactions among smart people and smart living dimensions with regard to privacy and security issues on OSN, while *Section 4* reveals the behavioral patterns of individuals on OSN. *Section 5* proposes the relationship model of privacy and security threats and presents some countermeasures regarding data protection and OSN that can lead to the development of safer and more ethical cities by improving the dimensions of smart people and smart living. An empirical study, which proves the proposed relationship model is presented in *Section 6*, while the paper concludes with *Section 7*, which contains some conclusions and future perspectives.

2. OSN impact on smart cities

This section presents the conceptualization of SC and discusses the exploitation of OSN in SC and their privacy and security risks, which undermine their significant contribution as urban data sources.

2.1. Smart city: a system of subsystems

Several definitions, conceptual architectures and models that approach SC from various perspectives have been proposed by SC scholars (Anthopoulos, 2017; Giffinger and Gudrun, 2010; Batty et al., 2012;

[1] http://www.itu.int/en/ITU–T/focusgroups/ssc/Pages/default.aspx.

Albino et al., 2015; Komninos, 2013) and standardization organizations (e.g., the International Standards Organization,[2] the International Telecommunications Union (ITU), etc.), with the purpose of clarifying organizational and implementation issues (ISO, 2015). For the purposes of our research, a technical model proposed by British Standard Institution (BSI, 2016) was selected, as it highlights the value of data, IoT and OSN in the SC implementation. According to BSI's model, SC is a system that consists of several subsystems (infrastructure–based sectors and service–based sectors), which interact via ICT (Fig. 1). In this model heterogeneous data is produced and collected via sensors from different hard facilities (energy, water, transport and waste) or in service–based sectors (health, education, safety and OSN); it is stored in city data storages; analyzed; and displayed on city dashboards. Embedded networks of sensors and devices in the physical space of cities and the new capabilities offered by OSN, Web 3.0 applications and crowdsourcing are expected to create a real-time spatial intelligence with a direct impact on the services that cities offer to their citizens (ISO/JTC, 2015).

2.2. OSN as sensors of urban dynamics

OSN (e.g., Facebook, Twitter, Foursquare, Instagram, etc.), as derived from the BSI's model, are one of the service-based sectors' subsystems that interact with other subsystems and contribute to the development and implementation of SC (BSI, 2016). These interactive computer-mediated technologies contribute to collective intelligence through crowdsourcing platforms, mashups, web-collaboration, and other means of collaborative problem solving (ISO/JTC, 2015). According to ISO/CD 37122 (ISO/TC 268, 2017), OSN are an excellent tool for the interaction between citizens and local authorities, as strengthen citizens' engagement and improve the management of non-emergency situations (e.g., complaints registration, brain storming for local issues, etc.). Examining their impact on e-government and e-participation, Dameri and Ricciardi (2014) concluded that OSN significantly contribute to: *i) service delivery*, *ii) governance participation*, *and iii) smartness awareness*.

In addition, OSN behave as “human sensors”, which record human activities and preferences (e.g., sentiment, political beliefs, social interactions, human mobility, presence in specific events, likes etc.) in cities (Moustaka et al., 2018a). Compared with sensor-based data collection methods, OSN offer: *i) volumes of heterogeneous data*, *ii) reduced costs*, *iii) interoperability*, *and iv) dependability* (Doran et al., 2014). The specific technical feature of OSN is that they offer the possibility of geolocation/check-ins, which facilitates the recognition of location based postings, expressions of interest and interactions, and by extension, the extraction of urban patterns that are useful for urban traceability and management. For instance, Aiello et al. (2016), extracted sound-related words from geo-referenced OSN content, which were retrieved by Freesound[3] and geo-tagged photos from Flickr, investigated the relationships between emotions and soundscapes for the cities of Barcelona and London and based on their findings characterized the areas of these cities as chaotic, monotonous, calm, and exciting (Fig. 2(a) and (b)). Also, Falher et al. (2015), used geo-tagged data (check-ins) from Foursquare and Twitter and discovered neighborhoods with similarities (e.g., areas with fashion shops, parks, government buildings, expensive residences, etc.) across cities in Europe and the USA, while Yang et al. (2018) have investigated human mobility at the community level in Wuhan with the analysis of geo-tagged data from Weibo (Fig. 3).

Twitter holds a prominent position among OSN as it offers: *i) real-time update*, *ii) flexibility*, *as a user can track someone else's post without being friends*, *iii) ability to harvest huge amounts of data through its APIs*, *and iv) potentiality for future situations prediction* (Bright et al., 2014; Hutchinson, 2016). With the use of geo-tagged data from Twitter, Doran et al. (2014) recognized and visualized various geographic, social, cultural and political characteristics that have led to the extraction of citizens' perceptual patterns in a large city. Efstathiades et al. (2015) identified users' key locations (i.e., home and work places) in Netherlands, city of London and Los Angeles county, while Gkatziaki et al. (2017) extracted urban social activity patterns and interactions, by modeling New York, London, and San Francisco cities into “dynamic areas” which are evolving over the time. Moreover, Kumar and Ahmed (2016) and Giatsoglou et al. (2015) exploited Twitter for traffic event detection and community detection, respectively.

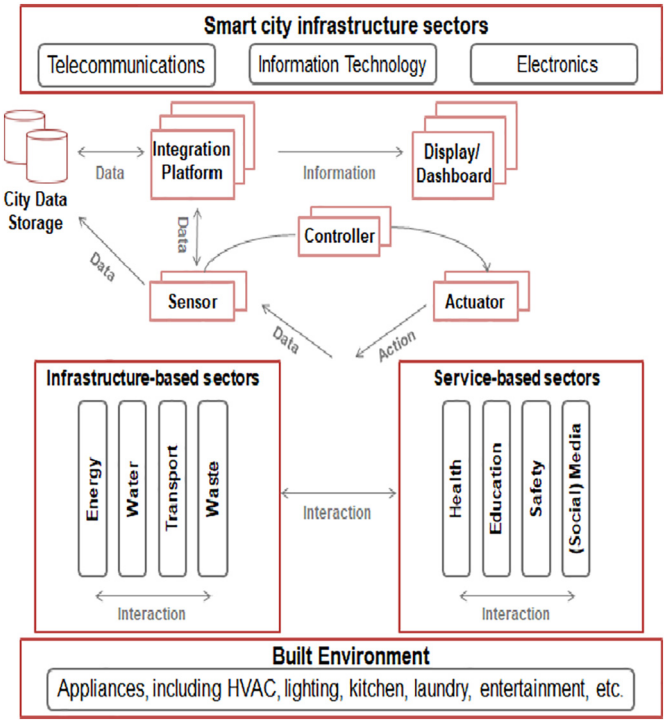

Fig. 1. Smart city and its subsystems (BSI, 2016).

Due to their advantages, OSN have already been widely utilized for the implementation of SC either independently or complementary to IoT (Doran et al., 2014; Martinez-Balleste et al., 2013; Mazhelis et al., 2016; Moustaka et al., 2018a; Solomon et al., 2016; Vakali et al., 2013). SC with interconnection of mobile devices that support the use of OSN and applications and IoT can collect and analyze data and improve the ability to extract patterns, and, forecast and manage urban flows and events.

2.3. OSN privacy risks & security threats

Despite the fact that OSN is a useful tool for SC stakeholders that exploit local data, many privacy and security concerns can be generated. 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, individuals' activities on OSN (e.g., social interactions, sentiments, personal preferences, location, etc.) are recorded and analyzed in their absence in SC (Martinez-Balleste et al., 2013; Rizzo et al., 2016; Luo et al., 2016). 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 individuals' personal information from the illegal disclosure and use by third malicious parties and it is directly related to the individual's online behavior and privacy

[2] https://www.iso.org/home.html.
[3] https://freesound.org/.

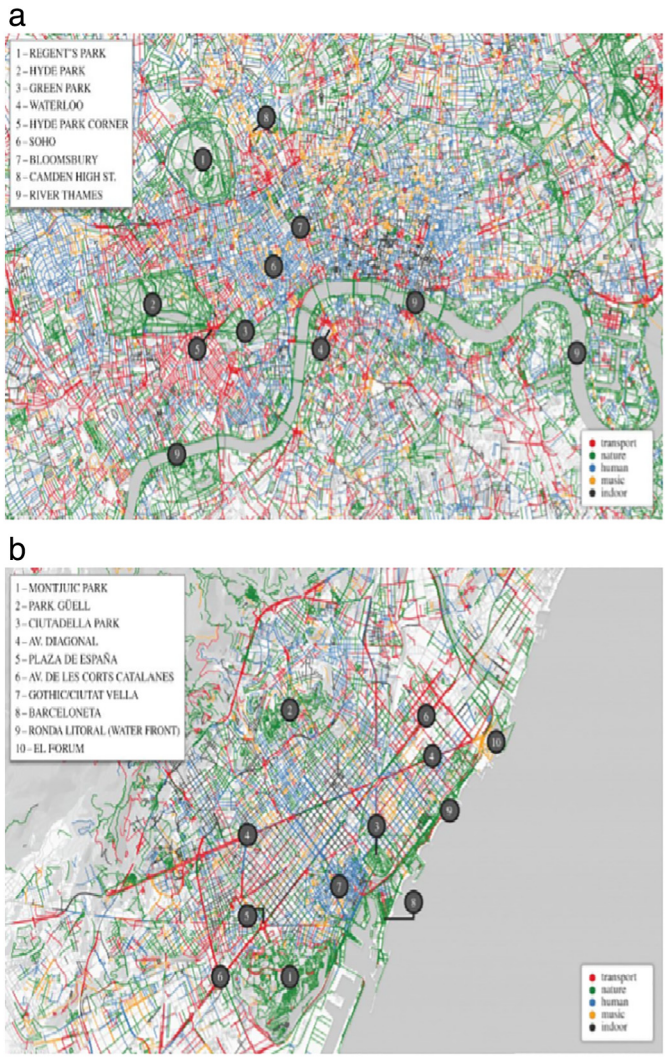

Fig. 2. (a): Urban sound map based on OSN data in London (Aiello et al., 2016) (b): Urban sound map based on OSN data in Barcelona (Aiello et al., 2016).

preferences (Zhang and Sun, 2010; Martinez-Balleste et al., 2013; Patsakis et al., 2014; Kitchin, 2016). Recent studies have revealed that individuals' belief that their privacy is more protected than that of others, and the degree of their trust in other users, compromise their privacy (Baek et al., 2014; Bergström, 2015). According to Solove's taxonomy, the privacy breaches and harms in SC occur and fall into the following four processes: *i*) *information collection*, *ii*) *information processing*, *iii*) *information dissemination*, and *iv*) *invasion* (Solove, 2006). Zhang and Sun (2010), in their work, have shown that individual's privacy on OSN is distinguished in three parts as follows:

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 on user's profile, in particular on the information and content that it is 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, 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 (Zhang and Sun, 2010).

Many research efforts have focused on identifying and dealing with risks and threats affecting OSN (Fire et al., 2014; Patsakis et al., 2014; Zhang and Sun, 2010). According to Fire et al. (2014), OSN threats can be divided into the following four main categories, the subcategories of which are presented in Fig. 4.

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 individual's 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. *Combined 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 they 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. The recent data scandal of Facebook and Cambridge Analytica that hit 78 million users is a prime example of the inadequacy OSN privacy and security settings, and the leakage and abuse of individuals' personal data (BBC, 2018; Groth, 2018). 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 (Patsakis et al., 2014).

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 (Fire et al., 2014). Parents cannot fully protect their children whose critical ability and online defense on OSN are limited, 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 (Minkus et al., 2015). The Canadian Centre for Child Protection[4] 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 cyberbullying[5] occurs mainly through OSN, while more than 82% of online sex crimes related to sexual predators[6] and online sexual offenses originate from OSN that predators use to gain insight into their victims. These threats can have disastrous and irreversible effects (e.g., suicides), as they greatly affect children's behavior and psychology (Fire et al., 2014; Minkus et al., 2015).

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

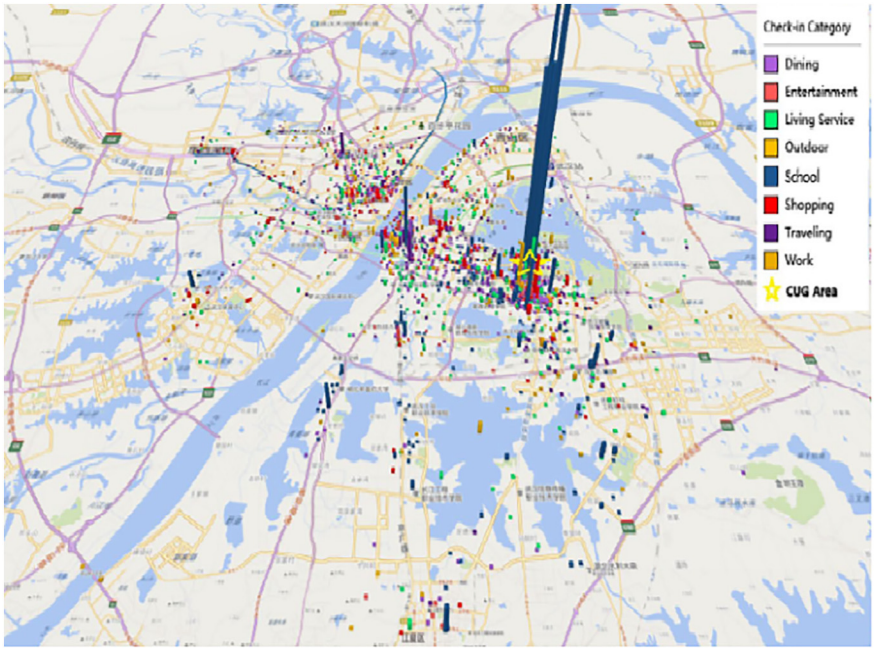

Fig. 3. The Weibo checking distribution in Wuhan (Yang et al., 2018).

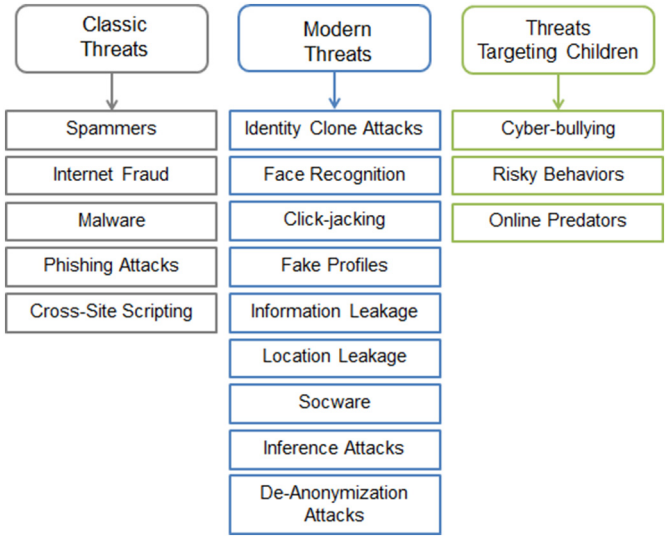

Fig. 4. Security threats on OSN (Fire et al., 2014).

3. Social dimensions vulnerabilities and interactions

Since OSN are directed and used by people and they influence life and security in cities, our study focus on *smart people* and *smart living* dimensions which are related to the social perspective of SC (Albino et al., 2015; Batty et al., 2012). The ISO/CD 37122 (ISO/TC 268, 2017) document concerns the *Sustainable Development of Communities in SC* and defines KPIs for the evaluation of these dimensions, the most relevant to our research of which, are presented in Table 1. With the purpose of focusing on the specific sub-dimensions of these two dimensions, which relate to privacy and security issues, we have exploited the appropriate smart people and smart living KPIs, which have been introduced by the ITU SC Focus Group. These KPIs comprehensively cover all aspects of life in SC in conjunction with ICT including safety and security issues such as the information security (ISO/IEC, 2015; ITU-T FG-SSC, 2014).

3.1. Smart people

People are recognized by many researchers as the main SC strength for SC infrastructure and service utilization (Bird, 2017; Giffinger and Gudrun, 2010; Marinaro, 2016; Nam and Pardo, 2011). In this regard, smart people SC dimension is being measured by the following indexes: i) *human factors*, which are *creativity*, *flexibility*, *social learning and education*, *level of qualification*, and ii) *social factors*, such as *social and ethnic plurality*, *open-mindedness* and *individuals' participation in public life* (Batty et al., 2012; Giffinger and Gudrun, 2010; Nam and Pardo, 2011). According to the ITU SC Focus Group, smart people fall into the dimension of *equity and social inclusion*. The degree of their "intelligence" can be measured by the corresponding KPIs, which evaluate: *i*) *education and training*, *ii*) *openness* (i.e., international communication and cooperation via ICT) and *iii*) *participation in public life* (ISO/IEC, 2015; ITU-T FG-SSC, 2014).

Individuals share their opinions, feelings and content on OSN, generate data with personal IoT devices (e.g., wearable, smart meters in their homes, health applications etc.), and in some cases participate in surveys and crowdsourcing activities (e.g., SEN2SOC[7] platform, CrowdFlower[8] platform, etc.). This data becomes a crucial city asset, since it can be transformed to valuable knowledge and helps decision-making (Moustaka et al., 2018a). If KPI values regarding education and training are high, it is expected that individuals possess advanced digital skills and to be responsible with OSN use and their personal data, which influences the local quality of life accordingly (ISO/IEC, 2015; ITU-T FG-SSC, 2014). Privacy, which is primarily personal responsibility, is ensured by the proper use of OSN privacy settings and can lead to security protection and improvement, as individuals cease to be vulnerable to malicious third parties. Mazhelis et al. (2016), in their work, have claimed that individuals' engagement can be enhanced, if they feel safe and convinced that their personal data, which are being recorded by the various devices and applications are fully protected and that they control the purpose of its use. Consequently, the feeling of security and confidence on OSN, encourages individuals to engage in social issues and this response increases the corresponding KPI values

[7] http://smartsantander.eu/index.php/sen2soc.
[8] https://www.crowdflower.com/.

Table 1
Association between smart people and smart living KPIs, focusing on security and social issues.

ISO/CD 37122 (ISO/TC 268, 2017)	Scholars (Giffinger and Gudrun, 2010; Nam and Pardo, 2011; Batty et al., 2012)	ITU SC Focus Group (ITU-TFG-SSC, 2014)
Culture	**Smart people**	**Smart people**
- Number of library book titles per 100,000 population	**Human factors**	- Education & Training
- Number of library e-book titles per 100,000 population	- Creativity	- Openness
- Active library users as a percentage of total population	- Flexibility	- Participation in public life
Economy	- Social learning & Education	
- Percentage of local businesses contracted to provide city services which have data communication openly available	- Level of qualification	**Smart living**
- Percentage of labour force employed in the ICT sector	**Social factors**	- Quality of life
Education	- Social & Ethnic plurality	- Physical Infrastructure
- Number of online databases available through public libraries per 100,000 population	- Open-mindedness	- Equity & Social cohesion
- Number of computers, laptops, tablets, or other digital learning devices available per 1000 primary school students	- Individuals' participation in public life	- Safety & Security (Information Security)
- Number of computers, laptops, tablets, or other digital learning devices available per 1000 secondary school students	**Smart living**	
Governance	- Cultural facilities	
- Annual number of online visits to the municipal open data portal per 100,000 population	- Health conditions	
- Number of datasets offered on the municipal open data portal per 100,000 population	- Individual safety	
- Percentage of municipal datasets available to the public	- Housing quality	
- Percentage of city services accessible online	- Education facilities	
- Average response time to relevant inquiries made through the city's nonemergency inquiry system (days)	- Touristic attractivity	
Recreation	- Social cohesion	
- Percentage of public recreation services that can be booked online		
- Number of municipal smart kiosks installed per 100,000 population		
Safety		
- Annual number of social media posts by municipal public safety officials per 100,000 population		
Telecommunications		
- Percentage of the city population with access to computers or other electronic devices with internet access in libraries and other public buildings		
- Percentage of the city population with access to sufficient speed broadband		
- Percentage of city area with publicly available internet connectivity		
Urban planning		
- Annual number of citizens engaged in the planning process per 100,000 population		

(i.e., *openness*, *participation in public life*), while it enhances service co-creation with local authorities (Lee and Lee, 2014; Zoonen, 2016).

On the contrary, low KPI values in smart people dimension (i.e., due to the lack of education and training, are expected to depict that individuals' OSN behavior is vulnerable to privacy and security threats (Cecere et al., 2015; Fire et al., 2014). Thus, malicious actors have an increasing opportunity to perform cyber-attacks, degrading OSN security and threaten OSN users. Moreover, user concerns regarding privacy violations and improper data tracing and use by third parties, discourage their OSN engagement and lead to registration of inaccurate and even wrong data (Kantarci and Mouftah, 2014; Zoonen, 2016). As a parallel effect, user participation in social issues is impacted and corresponding KPI values can decrease too.

3.2. Smart living

Smart living SC dimension depicts the local quality of life (Anthopoulos, 2017; Batty et al., 2012; Giffinger and Gudrun, 2010; Moustaka et al., 2018a) and it is being measured by the following indexes: *i*) *cultural facilities*, *ii*) *health conditions*, *iii*) *individual safety*, *iv*) *housing quality*, *v*) *education facilities*, *vi*) *touristic attractivity and vii*) *social cohesion* (Giffinger and Gudrun, 2010). ITU SC Focus Group has associated smart living with three of the six KPI dimensions, which are i) *equity and social cohesion*, *ii*) *quality of life* and *iii*) *physical infrastructure*, which are being measured by corresponding indexes (ISO/IEC, 2015; ITU-T FG-SSC, 2014). The proposed KPIs cover a wide range of services, from network and information facilities to health and education services.

Due to this SC dimension's broad scope, large amounts of urban data are required to understand local needs and develop and manage smart services (Anthopoulos, 2017; Moustaka et al., 2017; Moustaka et al., 2018a). Since the urban data that is collected from all the available data sources is circulated rapidly, new privacy and security concerns can emerge, which affect smart living KPI values regarding *safety and security*, and more specifically *information security* (ISO/IEC, 2015). Potential cyber-attacks to SC resources (e.g., databases, IoT networks, applications, etc.) and OSN (as it was described in Section 2) affect public security and privacy, as well as, openness and social participation, and in this respect they reduce corresponding smart living and smart people KPIs (Ahmed et al., 2014; Bartoli et al., 2011; Beltran et al., 2017; Elmaghraby and Losavio, 2014; Martinez-Balleste et al., 2013; Mazhelis et al., 2016; Solomon et al., 2016; Zoonen, 2016).

Consequently, the smart living KPI values demonstrate the levels of information security, openness and participation in public life, and determine the quality of life and citizen participation.

3.3. Individual privacy VS global security

In recent years, several standardization bodies (e.g., ITU, ISO, etc.) and scholars, approaching SC from different perspectives, have proposed sets of KPIs for the assessment of their performance. KPIs that indicate the level of smart people and smart living in terms of protecting their privacy, security and participation in public life are presented in Table 1. The International Standard *ISO/CD 37122* (ISO/TC 268, 2017) proposes a set of specific indicators for the evaluation of city services, such as culture, governance, telecommunications, etc. Indicators on education, culture and telecommunications services reflect "education and capacity building" issues and contribute to "social cohesion", "well-being", "resilience" and "attractiveness" purpose of the city as defined in ISO 37101 (ISO/TC 268, 2017), while urban planning and governance services reflects "empowerment and engagement" issues and contribute to "social cohesion", "attractiveness" and "resilience" purpose of the city. Finally, indicators for economy and recreation reflect "living together" and "living environment and working" issues and contribute to "social cohesion", "attractiveness", "resilience" and "well-being" purpose of the city (ISO/TC 268, 2017). Although ISO/CD 37122 (ISO/TC 268, 2017) introduces KPIs for education and capacity building, engagement and social cohesion issues, it does not provide indicators for assessing information security. On the other hand, the indicators proposed by SC scholars are suitable for understanding the SC dimensions, but are generic and overlapped by the official KPIs of the standardization bodies. Finally, the KPIs proposed by ITU SC Focus Group, which refer to all SC services from a technical point of view, with particular emphasis on ICT, were considered the most suitable for our research. The matching of these KPIs to privacy and security threats in OSN and the interactions between them are demonstrated in Fig. 5, in which red and green beats indicate direct and indirect interactions respectively.

According to the aforementioned two subsections and existing studies (Moustaka et al., 2018b), it appears that there is a strong interaction and correlation between smart people KPIs and smart living KPIs (i.e., information security, openness, public participation). Privacy protection at individual privacy levels can affect global security levels in cities and vice-versa, as it is depicted in Fig. 6. More specifically, the level of local education and training, and of openness determines their behavior and attitudes towards data provision and privacy concerns, while it affects positively or negatively information security in SC.

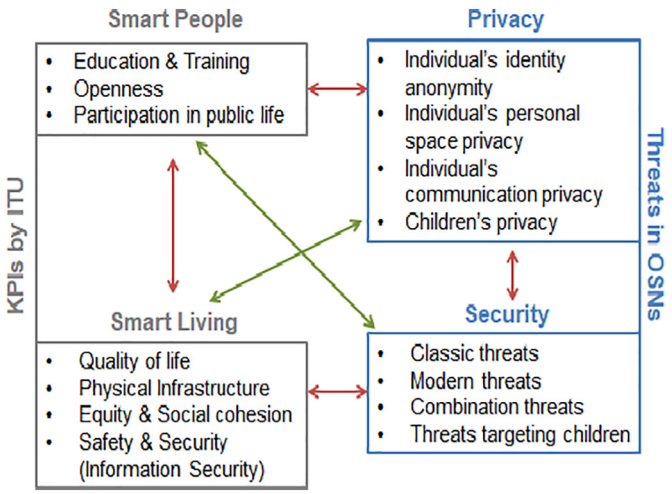

Fig. 5. Relations between KPIs and OSN threats.

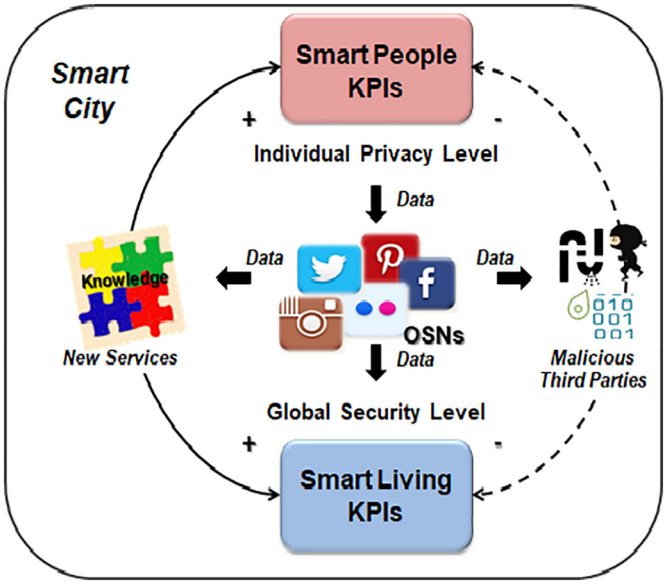

Fig. 6. "Privacy VS Security" in smart cities.

Moreover, data that is generated by participation activities is transformed into valuable knowledge for cities, which in turn leads to the development of new services; to the improvement of the quality of life and, finally, the enhancement of smart living.

On the other hand, in a "closed" SC, citizen attitudes and privacy concerns are influenced by the prevailing public perceptions and the level of information security, openness and quality of life. Individuals often lose their online trust, due to both their private and public concerns with regard to personal data trace and misuse, as it is depicted in Fig. 6. Mistrust and suspicion towards OSN discourage social participation and favors the entry of fake data, which in turn affects social engagement and decreases the corresponding KPIs. On the contrary, appropriate training activities, policy-making and campaigns can be undertaken by local governments, while the development and dissemination of privacy protection tools, can lead to behavior patterns social participation (Zoonen, 2016).

4. Behavioral patterns and phenomena over urban OSN

The determination of OSN behavioral patterns can become a useful tool for the realization of corresponding user activities. In this respect, and in an attempt to enhance OSN users' behavior and empowerment of smart people, as well as to revise the OSN operational context (e.g., privacy and security settings, data management, etc.), relevant empirical studies, which explore -from different perspectives- the participation motivations, the concerns and the behavior of different users in social networking are presented. Literature findings show that individuals' behavior on OSN can be organized in four stages, as follows: i) *Stage 1*: factors that motivate involvement; ii) *Stage 2*: privacy concerns; iii) *Stage 3*: individuals' behavior when using OSN; and iv) *Stage 4*: individuals' behavior when facing privacy and security risks. These stages are described in the following subsections.

4.1. Stage 1: involvement incentives on OSN

Social Web and its applications have revolutionized the Internet and they change the communication methods radically, while they enable dynamic interactions between users and organizations. It is remarkable that Facebook Messenger and WhatsApp alone handle more than 60 billion messages per day (Smith, 2016). Beyond direct communication (mobile messaging), Social Web delivers services that fulfill a rich variety of social and commercial needs, such as information crawl,

Fig. 7. Social Media Landscape (Cavazza, 2017).

publishing, sharing, networking, collaborating, etc., as it is depicted in Fig. 7. In this figure, Facebook, Twitter and Google are located in the center of the social ecosystem, as all the online services are being evolved around them (Cavazza, 2017). Recent records have revealed that approximately 510,000 comments are posted, 293,000 status changes are registered, and 136,000 photos are uploaded on Facebook every 60 s; 500 million Tweets are sent every day; 3.5 billion likes/day are taken place on Instagram; and 56 million blog posts are published on Wordpress every month (Smith, 2016; ZEPHORIA, 2017). Although the use of OSN for commercial (Bertot et al., 2012; Kim et al., 2015) and governmental purposes (Hanna et al., 2011; Schivinski and Dabrowski, 2016) is comprehensible, questions arise with regard to the reasons and incentives of the increasing involvement of individuals on OSN.

The direct, multimedia, and cost-effective way of communication, appears to be a profound reason, but only for users that eagers them to create and share content, and sometimes valuable private information on OSN. There are more complex reasons that justify this behavior (Yin et al., 2015; Gangadharbatla, 2008; Kisekka et al., 2013; Ball et al., 2015). Yin et al. (2015) explore the key factors that affect users' continuous intention of using OSN and they discovered that *fear of missing out* (FoMO) and *fun* positively affects a continuous OSN use. These findings were verified by a recent social research which, focusing on investigating and identifying the 10 most popular reasons for using the OSN, revealed that 42% of Internet users use them to "stay in touch with what their friends do", while other popular reasons are real-time updates, free time spending, social networking, and content and opinion sharing (McGrath, 2017). The same survey also showed that people of 16–24 year-olds use social media to fill up spare time, users among 25–34 year-olds to stay in touch with their friends, and users among 34–44 year-olds to stay up-to-date with news and current affairs. Therefore, the reasons for using OSN and users' expectations vary depending on their *age*. The same conclusion is reached by Kisekka et al. (2013), who, after adopting the Communication Privacy Management (CPM) theory and using a sample size of 488 adult Facebook mobile phone users, have investigated the differential impact of age on the extent of Private Information Disclosure (PID). Their findings demonstrate that i) likelihood of PID was less for three groups of users: females, individuals who use smartphones to access their accounts, and individuals with more than one active OSN account; ii) usability affected older and younger adult users differently; and iii) an increase in social networking involvement does not increase the likelihood of PID. Findings vary with regard to the role of *gender* too. A few scholars have claimed that gender does not influence individuals' practices (Furnell, 2008; Levy and Ramim, 2009), while others such as Fogel and Nehmad (2009) argued that gender affects individuals' online personal information sharing practices. The above findings justify that the reasons, which motivate individuals to use OSN are determined by *demographic factors* such as age, gender, and education. Focusing on *psychological factors*, *Internet self-efficacy*, *need to belong*, and *collective self-esteem* all have positive effects on individuals' attitudes towards OSN. Specifically, the individual's attitude towards OSN mediates the relationship between his willingness to join OSN and i) Internet self-efficacy and ii) need to belong, while the mediation is only partial between his willingness to join and collective self-esteem (Gangadharbatla, 2008). Furthermore, Ball et al. (2015), assessing and comparing the influence of individuals' personal information sharing awareness (PISA) on their habits (PISH) and practices (PISP) on OSN, has demonstrated that individuals' habits were determined to have the strongest influence on their practices and information sharing activities, while the awareness was not significantly influencing them.

4.2. Stage 2: individuals' privacy concerns

OSN are very popular as more and more people spend more or less time on them. Despite widespread warnings regarding dangers of poor online security practices, a surprisingly high percentage of users remain still very naive about security on OSN (Jang-Jaccard and Nepal, 2014; Sundar and Marathe, 2010). Since incentives for OSN use differ, privacy concerns, trustiness and individuals' behavior towards them also vary. A lot of individuals take into account OSN risks and adhere to necessary security settings, while other individuals are clueless and exposed directly to underlying risks. According to "privacy paradox", individuals with high level of privacy concerns are more vulnerable to personal data disclosure, while there is inconsistency between privacy concerns and privacy settings (Acquisti, 2010; Acquisti and Gross, 2006; Norberg et al., 2007). Of particular interest are the findings of Hoadley et al. (2010) who ascertained that easy information access and "illusory" loss of control on Facebook prompted by the introduction of News Feed features trigger privacy concerns to its users. Actually, individuals' privacy perceptions and concerns are affected by various *socio-demographic*, *psychological* and *cultural factors*. Acquisti and Gross (2006) and Cecere et al. (2015) found that males are less concerned than females regarding online privacy, Jensen et al. (2005) claimed that women are more hesitant than men, while other empirical studies revealed that there is no significant difference between two genders (Sheehan, 2002; Yao et al., 2007). Moreover, Yao et al. (2007) revealed that beliefs in privacy rights, as well as psychological needs for privacy are the main influences on online privacy concerns. With regard to age and education, relative studies have concluded that both of them have positive impact on individuals' privacy concerns (Bellman et al., 2004; Brown and Zukowski, 2007; Cecere et al., 2015; O'Neil, 2001; Sheehan, 2002). Finally, Cecere et al. (2015) the level of individuals' privacy concerns is determined by both cultural and socio-demographic factors. Specifically, analyzing data from a survey drawn up for EU, they found that Northern and Eastern European countries are less concerned about the misuse of personal data than Central and Southern European countries, while at the individual level, the results demonstrate that women, highly educated and middle-aged individuals are more concerned about potential personal information misuse than other individuals' groups.

4.3. Stage 3: individuals' behavior on OSN

The individuals' behavior on OSN is often unpredictable and reflects both their privacy concerns and their personalities. Several studies have concluded that different types of information have different levels of sensitivity, while individuals are less likely to disclose more sensitive information. Consolvo et al. (2005) and Lederer et al. (2003) both

found that individuals are more willing to share vague information than specific personal information, while Gross and Acquisti (2005) identified incomplete information, bounded rationality, and systematic psychological deviations from rationality as three main challenges in privacy decision making. Moreover, Knijnenburg et al. (2013) claimed that individuals' disclosure behavior is in fact multi-dimensional as different people have different tendencies to disclose various types of information, while Norberg et al. (2007) have considered that most OSN users share content and personal information much more freely than expected based on their attitudes.

OSN offer users the ability to manage the information they disclose and protect their privacy through their privacy settings (Kuczerawy and Coudert, 2011). Since the right implementation of privacy and security settings is user-dependent and indicates individual's behavior on OSN, several studies have been conducted to investigate the suitability and reliability of privacy settings, as well as individuals' behavior regarding their proper selection and use (Hugl, 2011; Kuczerawy and Coudert, 2011; Li et al., 2015; Madejski et al., 2011; Stross, 2009). According to Kuczerawy and Coudert (2011) and Stross (2009) only 25% of Facebook users have changed their privacy settings, while the majority of Facebook users are not properly informed about them. Li et al. (2015), by examining representative OSN including Facebook, Google, and Twitter, discovered that there are conflicts between privacy control and OSN functionalities, so that the effectiveness of privacy control may not be guaranteed as most OSN users expect. Moreover, Luo et al. (2011) in their work have quantified the disparity between the desired and actual privacy settings and found that users' privacy settings match users' expectations only 37% of the time, while often they share more information than expected. Madejski et al. (2011), evaluating the actual preferences and behavior of Facebook users, found that there is a lower limit of the inconsistencies between users' sharing intentions and their privacy settings. In some cases individuals, depending on privacy settings of their online friends, can make their friends and the network of their friends vulnerable on Facebook risks (Gundecha et al., 2011). Additionally, Netter et al. (2013) studying the privacy settings on OSN with the use of a novel approach based on profiles content of Facebook users, have indicated a mismatch between perceived, preferred, and actual settings due the lack of users' awareness and control. Finally, Aljohani et al. (2016), conducting a survey on OSN users' privacy settings and information disclosure and investigating users' behavior on Facebook, Twitter, Instagram, and Snapchat, found that huge amounts of personal information are revealed at different levels between OSN, and actually, the *socio-demographic factors* such as gender, age, and education significantly affect information disclosure and privacy settings use. Therefore, the existence of privacy settings does not guarantee individuals' protection on OSN, but their proper use is required, which depends on individuals' online behavior determined by their background.

Of particular interesting are two comprehensive studies that explored the personal (i.e., education, experiences, maturity, awareness, etc.) and psychological factors that affect individuals' behavior on OSN. Shillair et al. (2015) using the protection motivation theory (PMT), a model within the class of social cognitive theories (SCT), investigated the interaction among user knowledge, personal responsibility, and training techniques for the purpose of encouraging online safety behavior. Their findings have shown that the above factors interact with each other as follows: enhancing individuals' sense of personal responsibility can lead to the adoption and implementation of appropriate and effective internet security measures, but it is not always sufficient. The measures taken and the training of individuals should match their level of knowledge in order to improve their online behavior. On the other hand, Dong et al. (2015), performing two common scenarios, information requests and information sharing, investigated the main psychological factors that influence privacy–making on OSN. The study outcomes are summarized as follows: i) information sharing is affected by the audience, while information requests depend on the requester as he/she determines the receiver's trust and the final privacy decision-making outcome, ii) individual's privacy decision-making on OSN depends mainly on the tradeoff between privacy and self-presentation, iii) sensitivity varies with audience, iv) contextual information should be taken into account for privacy decision-making, and v) individuals tend to share information or receive requests when conditions permit.

4.4. Stage 4: individuals' behavior when facing privacy and security risks on OSN

The individuals' behavior when they are confronted with privacy risks on OSN, as expected considering the above analysis, varies. An empirical study, conducted by Saridakis et al. (2016), aiming at investigating how individuals' online activity and perceptions of personal information security on OSN are related to their online victimization, has revealed that the latter is affected positively by: i) high OSN use, ii) low perceived risk, and iii) high risk propensity; and negatively by: i) high perceived control over information, and ii) high computer efficacy. Additionally, it was found that use of multipurpose OSN (e.g., Facebook, Google+, etc.) have a negative impact on individuals' victimization in contrast with OSN for knowledge exchange (e.g., LinkedIn, Blogger, etc.) which affect positively online victimization. Shin (2010) has also attempted to examine security, trust, and privacy concerns with regard to OSN among consumers, developing a novel model of trust-based OSN acceptance. His findings have revealed that: i) individuals are concerned about the vulnerability of security and privacy breaches when they use OSN, ii) perceived security and perceived privacy are directly associated with trust in OSN use, and iii) perceived security affects much more the individuals' attitude than perceived privacy. Moreover, Rauniar et al. (2014) investigated the individuals' attitudes towards OSN use proposing a revised Technology Acceptance Model (TAM) framework, and ascertained that perceived usefulness and trustworthiness of an OSN site determine the individuals' use intention of OSN, which in turn, affect the individuals' actual behavior on OSN.

The work of Angulo and Ortlieb (2015) is one of the very few efforts, which aims to reveal and identify common online privacy panic situations that individuals experience. The authors have investigated individuals' expectations and models of appropriate auxiliary mechanisms that could lead them towards a security solution, calming their anxiety, and preventing similar future situations, using a “virtual” privacy panic button. Their findings have shown that individuals are more concerned about potential harm to their finances or fear of discomfiture as well as third-parties knowing information regarding their personal life. Account hijacking and personal data leakage are the most frequently self-reported panic stories, while individuals are also worried about the loss of their mobile devices and their online data, the identity theft, etc. Finally, if the deployment and use of a virtual panic button was feasible, individuals would like the help provided to be immediate and effective.

4.5. Individuals' behavior formulation in SC

The previous analysis (Sections 2, 3 and subsections 4.1–4.4) and the assumption that individuals (users) are the main focus of privacy and security in OSN and SC (Marinaro, 2016; Bird, 2017) have led us to the design of Fig. 8. As shown, individuals are at the center of the circle, and their overall online behavior, which consists of four stages depicted in a different color, is determined by the current privacy and security conditions in OSN and SC. Fig. 8 combined with subsections 4.1–4.4 can be used as a useful tool for those who are interested in understanding the individuals' behavior on OSN, cultivating smart people and exploiting their contribution in SC. As revealed by the summary of subsections 4.1–4.4, the participation incentives, the individuals' concerns about security and privacy, and ultimately, the behavior of individuals on OSN, are determined by: *i) psychological* (*personal*) *factors* (e.g., level of individual's education, habits, self-esteem, self-

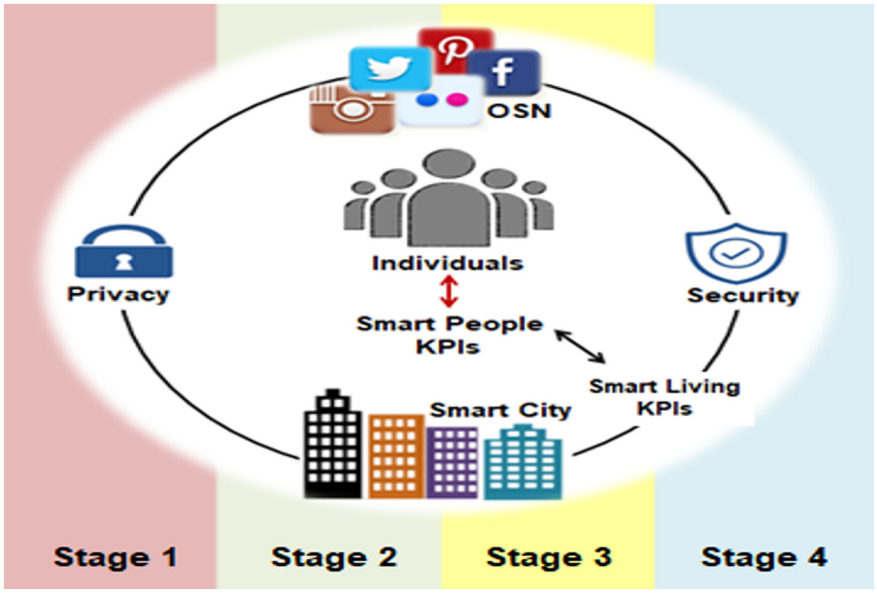

Fig. 8. Behavioral patterns in social networking.

presentation, personality, etc.), *ii*) *demographic factors* (e.g., age, gender, etc.), and *iii*) *socio-political factors* (e.g., legislation related to privacy and security protection, level of public education, city's or country's culture, etc.). Therefore, the level of information security, privacy and quality of life of SC is responsible for shaping the online behavior of individuals in all four stages, and for participating in public life through social networking. The openness and participation of individuals in public life (two of three smart people KPIs), regarding OSN exploitation, are influenced and determined by the level of their education and training (third smart people KPI), as well as by the smart living KPIs, discussed in Section 3. As a consequence, when the values of smart people and smart living KPIs are high, individuals' behavior on OSN is expected to be responsible and prudent, and beneficial to SC.

5. Dealing with privacy and security challenges in smart cities

Since civic engagement and exploitation of OSN are vital for SC shaping, particular attention should be paid to addressing privacy and security challenges related to OSN, with the aim of developing safe and ethical SC where people will feel protected, and cultivating smart people who will be actively involved in SC. Smart people KPIs and smart living KPIs, especially those related to education and training, openness and information security, are indicative of the level of privacy and security in a city. The achievement of high values of KPIs, which will lead to the enhancement of cities' and people's intelligence, requires: a) identifying and understanding the factors that affect individuals' behavior on OSN and SC (Section 4); b) the understanding of differences between privacy and security threats to identify vulnerabilities that facilitate the abuse of private data; and c) taking necessary measures (e.g., revision of privacy and security legislation, software tools, specialized training and education, etc.) to prevent and deal with them.

5.1. OSN privacy risks vs OSN security threats

The exploitation of existing literature (Fire et al., 2014; Minkus et al., 2015; Patsakis et al., 2014; Zhang and Sun, 2010) on privacy and security threats on OSN in conjunction with the identification of interaction among smart people KPIs and smart living KPIs regarding privacy and security in SC (discussed in Section 3), have led us to understand the differences between privacy and security threats and define the borderlines between them (Fig. 9). As demonstrated in Fig. 9, individuals' privacy on OSN is threatened by risks associated with their identity, profiles' content, and communication network information (Zhang and Sun, 2010). Moreover, risks that threaten children's privacy, which are a special case, have been also added. The security threats (Fire et al., 2014) caused by third parties and degrade the information security and 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. (2014) and how these attacks are correlated with the privacy threats (Zhang and Sun, 2010) 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 SC stakeholders who utilize OSN as an urban data source and care about individuals' security and engagement in SC. For instance, they can develop novel smart and specialized tools, software and applications to protect or educate individuals and children on OSN, improving both smart people KPIs and smart living KPIs.

5.2. Boosting participation on OSN

The excessive exposure of individuals especially children to ICT and OSN, the failure of OSN to protect effectively their users, and the lack of adequate and revised legislation increase the privacy and security risks and attacks in cities. (Li et al., 2015; Minkus et al., 2015; Patsakis et al., 2014; Shillair et al., 2015; Zhang and Sun, 2010). The adoption and implementation of new and appropriate measures are vital to protect the online activity of individuals and boost their engagement in SC. Some of the measures proposed by the existing literature, which need to be further enforced and enriched, are discussed below.

5.2.1. Education and training for secure behavior

Dealing with privacy and security threats depends mainly on individuals' personal background (e.g., personality, experiences, education, skills, etc.) (Cecere et al., 2015; Conteh and Schmick, 2016; Gangadharbatla, 2008; Saridakis et al., 2016), despite the fact that human factor is usually neglected in information security (Luo et al., 2011). As Conteh and Schmick (2016) have pointed out, individuals' vulnerability to cyber risks and attacks lies in human behavior and psychological predisposition, which can be influenced through education. In additions, Patsakis et al. (2014) have claimed that education combined with user awareness raising through applications'

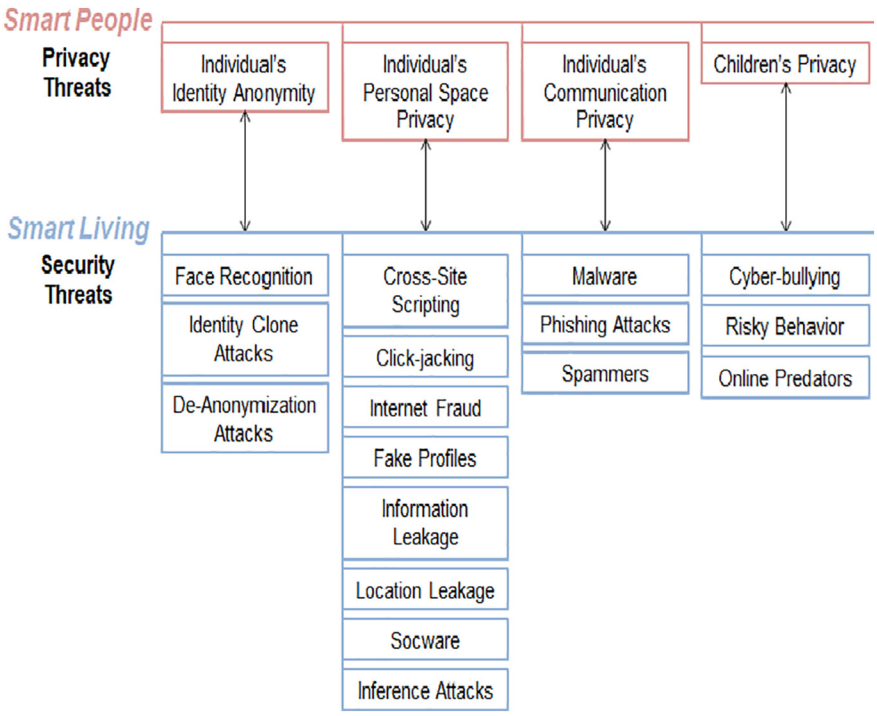

Fig. 9. Borderlines between privacy and security threats.

notifications can greatly enhance the online protection of individuals. Several researchers have focused on developing appropriate tools and programmes for educating and training individuals about the challenges of the Internet and OSN, recognizing the importance of education in individuals' personality and online behavior. Arachchilage et al. (2016) have developed a mobile educational game aimed at training individuals to be able to be protected from phishing threats, while Amosun et al. (2013) have designed and proposed a cybercrime prevention programme addressed to students, which can be used to foster the effective learning of cybercrime prevention. Finally, the work of Notar et al. (2013), a review of the literature for the period 2005–2013, summarizes all countermeasures developed and implemented in schools (e.g., public school sponsored programmes, curriculum based programmes parent programmes, online programmes, applications, etc.) for cyber-bullying intervention and prevention.

5.2.2. Tools and software for privacy and security protection

Beyond training, education and appropriate awareness, a variety methods and tools have been proposed and developed aiming at increasing the protection of privacy on OSN and "awakening" individuals (Li et al., 2015; Patsakis et al., 2014). Fire et al. (2014) in their work discussed OSN operator, commercial and academic solutions (e.g., OSN privacy and security settings, MinorMonitor, Defensio, socware detection, phishing detection, etc.), while Patsakis et al. (2014) 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[9]), and empower individuals to protect their photos online (e.g., Cryptagram) (Tierney et al., 2013). 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 ENCASE Project[10] context. 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 (Tsirtsis et al., 2016).

5.2.3. Data privacy legislative framework

Since targeted education and training and the development of appropriate tools are necessary but not sufficient conditions for the achievement of full protection of individuals on the Internet and OSN, the revision and enforcement of strict legislation to safeguard the privacy and security of individuals is required (Li et al., 2015; Minkus et al., 2015; Patsakis et al., 2014; Shillair et al., 2015; Zhang and Sun, 2010). Certainly, the legal framework and its implementation vary between different countries and geographical or federal unions such as the European Union (EU), the United States of America (USA), etc., but globalization and the lack of borders on the Internet lead to the need for overlaps between the relevant laws for the purpose of developing a unified international framework for trade and privacy protection (Robinson et al., 2009; O'Connor, 2018; Parsons, 2017).

Existing privacy laws have proved inadequate as they have not been able to prevent privacy violations and left many issues unregulated (Cobb, 2016; O'Connor, 2018; Parsons, 2017; Robinson et al., 2009). The European Data Protection Directive 95/46/EC, although considered to be an ideal reference model for the protection of personal data inside and outside the European Union, has exposed weaknesses in addressing: i) globalization, ii) the rapid evolution of technological capacity, and iii) the ways and purposes of personal data use (Robinson et al., 2009). With regard to the USA, Cobb (2016), conducting a review of the current US data privacy legislation in his work, concluded that US data privacy legislation tend to defend the trade interests as well as those of state security agencies and not the privacy interests of individuals. Finally, the Asia-Pacific region (APAC), trying to follow the rapid technological advancements and face the privacy and security risks, has proceeded with legislative reforms to revise existing legislation in 2016 (Parsons, 2017).

The EU, listening to the needs of an increasingly data-driven world, for the purpose of protecting all EU citizens from privacy and data breaches, has established the General Data Protection Regulation (GDPR), replacing the Directive 95/46/EC. The new regulation, which

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

is expected to become the "gold standard" all over the world and will come into force on 25 May 2018, is the first law that directly regulates the privacy of individuals by defining explicitly the context of processing and movement of personal data inside and outside the EU (EDPS, 2018; EU GDPR Portal, 2018). Compared with the previous Directive, the GDPR has broadened the territorial scope, has clearly defined the penalties and has strengthened the terms and conditions of consent. Moreover, the GDPR clearly defines the rights of individuals (subjects), which are: (i) notification of personal data breach, (ii) access to the data gathered and the manner and purpose of its use, (iii) right to delete data, (iv) data portability, and (v) data protection during collection and processing processes; while introduces and establishes Data Protection Officers (DPO), who are obliged to notify their data processing activities to local Data Protection Authorities (DPA) (EU GDPR Portal, 2018). The GDPR also places particular emphasis on the protection of minors by introducing for the first time the requirement of parental consent for the processing of personal data of children under the age of 16 (unless national laws set a lower age threshold which cannot be lower than 13) when information services are offered (Macenaite and Kosta, 2017).

The new European regulation is expected to form the basis for revision of the legislation on data privacy protection in other countries, on the one hand because it is comprehensive covering all privacy issues, on the other because it determines the compliance framework of foreign companies operating in the EU (Cobb, 2016; Parsons, 2017; Robinson et al., 2009). Notwithstanding the impact that the new regulation will have on the data exploitation for urban knowledge acquisition, it will certainly enhance individuals' privacy and security and will lead to the development of safer and more ethical SC in Europe (SCC Europe Staff, 2018; Valerio, 2018).

The study on exploring the privacy and security issues arising from individuals' social networking activities in the SC context let to the answers to research questions RQ1 and RQ2. The proposed model that specifies the relationships between the potential privacy and security threats on OSN, revealing individuals' vulnerabilities during their social networking activities, is the answer to RQ1. Behavioral patterns resulted from a brief literature review of empirical studies, which is presented in Section 4, are the answer to RQ2. Individuals' behavior on OSN is unpredictable as it determined by psychological, demographic and socio-political factors. SC stakeholders, leveraging these patterns, can better understand the individuals' multidimensional behavior in OSN in order to adopt and apply both personalized (e.g., education, tools, etc.) and universal (e.g., legislation, etc.) privacy and security protection policies in SC.

6. Research methodology: the smart city of Trikala

The proposed relationship model is tested and validated in this section. More specifically, an empirical study is performed, which concerns evidence from the SC of Trikala. Trikala is a typical medium-sized city that is located in the center of Greece, which became the first Greek digital city in 2004 and entered the list of 21 top SC in the world lately, (The Guardian, 2018). The city, adopted an architecture that follows the BSI model (Fig. 1), which consists of the following four Layers that interact with each other (Fig. 10):

- ***1st Layer***: Physical Environment;
- ***2nd Layer***: Telecommunications and Electronics (hard ICT facilities);
- ***3rd Layer***: Information Technologies (soft ICT facilities);
- ***4th Layer***: Infrastructure–based sectors and service–based sectors (end users and applications).

The *first Layer* concerns the physical environment and the utilities (i.e., people, buildings, vehicles, networks of electricity or water, etc.). The *second Layer* includes telecommunications and electronic infrastructures (i.e., CCTV systems, IoT, etc.), which are necessary to collect and store data, while the ICT infrastructure (i.e., databases, Geographic Information System (GIS), Cisco Smart and Connected Digital Platform (Kinetic), etc.) are located in the *third Layer*, where the data storage, process and control of (all coming from the second and fourth layers) are carried out. The *fourth Layer* includes all the smart services that have been deployed in the city: such as e-KEP (citizen self-service center); metro WiFi with a simple social logger; city's official App (TrikalaCheckApp) (i.e., for complaints registration and information retrieval); smart lighting and smart parking systems; tele-care services, etc. are only some of the available smart services in the testing case (Smart Trikala, 2018). OSN (e.g., Facebook, Youtube, Instagram, etc.,) are being used by the municipality as an alternative channel to connect with the citizens and they are also mentioned in the *fourth Layer*. Data flow occurs between all the architecture layers.

These smart services and applications are being used frequently and some privacy and security threats concern the following three use-cases:

- ***1st Use Case – TrikalaCheckApp***: user registration requires personal information sharing (e.g., name and email) or alternatively, users can authenticate with their OSN profile. User registration and authentication are necessary to ensure the Municipality for complaints' validity, but the process collects data for various purposes such as, statistics, urban insights, municipal response, quality of service measurement, etc. Privacy risks, which threat individual's identity anonymity, personal space privacy, and communication privacy, occur in this service (Layer 4) as the user's name and electronic/social identity are disclosed.
- ***2nd Use Case – metro WiFi Access***: the city offers free-of-charge Wi-Fi accessibility, which requires user registration and authentication with a similar to the previous process. Personal data (social profile) is being stored on the Wi-Fi Data Logger that the city collects and analyzes for safety (cyber-attack avoidance) and even marketing reasons. Similar to the previous use-case's privacy and security threats can be considered too.
- ***3rd Use Case – Malicious Attacks on IT Infrastructures and Services***: These attacks, which may affect any of Layers 2, 3 and 4, come from malicious third parties and fall into security threats (see Subsection 2.3).

Therefore, citizens (individuals) are responsible for the protection of their privacy in the first two use-cases, while the city is responsible for protecting the infrastructure and its citizens from the attacks of malicious third parties in the third case.

The Municipality of Trikala respects these risks, since the loss of privacy through smart service execution can affect citizens' participation and in order to establish a high level of *information security* in IT infrastructures and smart services, has undertaken the following training actions that address user skills:

- A branch of "Tech Talent School",[11] with the support of the Microsoft YouthSpark initiative has been setup and offers courses that enhance digital skills for adults and unemployed;
- A branch of Cisco Certified Local Academy has been founded, which offers several certification programs to professionals;
- Numerous competitions and workshops take place in the city, such as CodeGirl,[12] EducationRobotics,[13] Datathon, CodeWeek, etc., to inform, engage and train children;
- The ICT infrastructure and the smart services are being monitored by a control room in the Town Hall where data collection and

[11] http://techtalentschool.gr/en/information/.
[12] https://trikalacity.gr/to-prototypo-programma-codegirls-sta-trikala/.
[13] http://www.trikalarobotics.gr/.

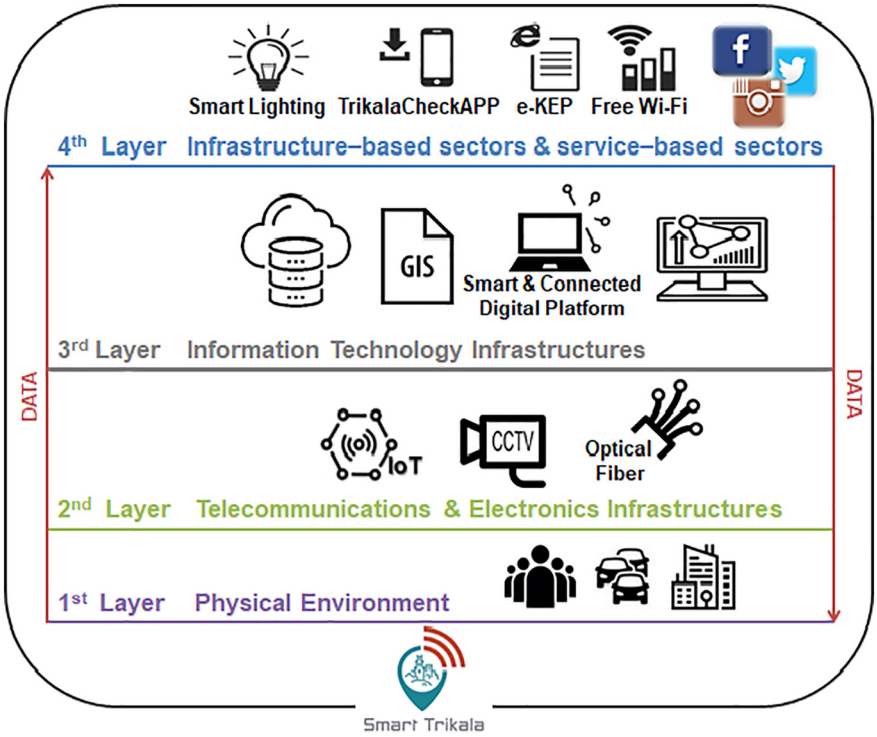

Fig. 10. The architecture of Smart Trikala.

processing is performed;
- Municipal services operate in compliance with the GDPR regulation.

The above brief presentation of the smart Trikala case, shows that the city pays significant attention on the smart people KPIs, which reflect the individuals' engagement, openness and education, as well as the smart living KPIs referring to life quality and information security.

7. Conclusions & future perspectives

This article deals with security and privacy issues on OSN and investigates how these affect and relate to smart people and smart living dimensions, with the purposes of: i) encouraging the use of OSN as an urban data source in the SC context, ii) helping the transformation of individuals into smart people, and iii) contributing to the formation of safer and more ethical SC. The proposed relationship model along with behavioral patterns, which provide with answers to RQ1 and RQ2 and it is demonstrated by an empirical study on the Trikala city, is expected to be beneficial to privacy and security protection over OSN use in SC.

The completion of the study led to the answers to the research questions RQ1 and RQ2. Specifically, answering to RQ1, the main vulnerabilities that lie behind individuals' activities in OSN in SC are the risks that threaten individual's identity anonymity, individual's personal space privacy and individual's communication privacy, as well as the security threats caused by third parties (i.e., classic threats, modern threats, etc., – discussed in Subsection 2.3). These vulnerabilities significantly affect the smart people and smart living KPIs that are indicative of each smart city's performance. With regard to RQ2, SC stakeholders aiming at enhancing the protection of individuals during social networking and encouraging their participation in SC in order to design and implement appropriate policies should take into account the four stages of individuals' behavior on OSN presented in Section 4. Psychological, demographic and socio-political factors are crucial for the formation of the individuals' behavioral patterns in both social networking and in SC.

The analysis has demonstrated a strong interaction between smart people KPIs and smart living KPIs, as the degree of privacy protection determined by the level of education and training and openness affects the security levels in SC which in turn determines the degree of individuals' participation in public life. Consequently, privacy protection at individual privacy level (smart people) can drive to global security level (smart living) in SC, and vice-versa. Moreover, the study of users' behavior on OSN has revealed that individuals' behavior is often unpredictable, while the chaotic nature of the Internet and OSN combined with new threats emerging by skipping the protection tools, which have already been developed, expose individuals to privacy and security risks, degrading information security, and their participation is public life. The exploitation of behavioral patterns in social networking and of proposed relationship model which specifies the borderlines between privacy and security threats, along with some appropriate measures and the enforcement of GDPR expected to lead to the successful treatment of privacy and security issues and cultivation of smart people, who will contribute effectively to improvement of life quality in cities.

The limitation of this work is that the current empirical study investigates only three use-cases, concerning security and privacy threats to demonstrate the model and interactions between smart people and smart living KPIs and threats in OSN. Nevertheless, they are representative use-cases that normally occur in all SCs around the world.

Some future thoughts concern that we plan to expand our work by designing and proposing smart people KPIs, which will be appropriate for measuring and evaluating the level of digital education and behavior of individuals regarding OSN and IoT use in the SC context. These KPIs, along with existing indicators that assess individuals' participation in public life, will provide an overview of the level of smart people maturity regarding the exploitation of ICT for knowledge acquisition and smart services development in SC. Another future thought is the accurate measurement of the correlations between the aforementioned smart people KPIs and the smart living KPIs, with regard to the information security, in order to enable the objective evaluation, comparison and ranking of cities. Finally, it would be of particular interest to study the privacy and security issues that are related to children's life in the SC context, as they are a sensitive age group of smart people,

which will determine the future evolution of SC.

Acknowledgments

This work is supported by the European Union Horizon 2020 - Research and Innovation Framework Programme under the Marie Skodowska-Curie grant agreement No 691025.

References

Acquisti, A., 2010. The economics of personal data and the economics privacy, OECD working articles WPISP and WPIE. Available at: http://www.oecd.org/dataoecd/8/51/46968784.pdf, Accessed date: 20 March 2018.

Acquisti, A., Gross, R., 2006. Imagined communities: Awareness, information sharing and privacy on the Facebook. In: Proceedings of 6th International Conference on Privacy Enhancing Technologies (PET'06), https://doi.org/10.1007/11957454_3.

Ahmed, K.B., Bouhorma, M., Ahmed, M.-B., 2014. Age of big data and smart cities: privacy TradeOff. IJETT 16 (6) (Oct. 2014. Retrieved, Dec. 2017, from). https://arxiv.org/ftp/arxiv/papers/1411/1411.0087.pdf.

Aiello, L.M., Schifanella, R., Quercia, D., Aletta, F., 2016. Chatty Maps: Constructing Sound Maps of Urban Areas From Social Media Data. The Royal Society Publishinghttps://doi.org/10.1098/rsos.150690.

Albino, V., Berardi, U., Dangelico, R.M., 2015. Smart cities: definitions, dimensions, performance, and initiatives. J. Urban Technol. 22 (1), 3–21. https://doi.org/10.1080/10630732.2014.942092. (February 2015).

Aljohani, M., Nisbet, A., Blincoe, K., 2016. A survey of social media users privacy settings & information disclosure. In: Johnstone, M. (Ed.), Proceedings of 14th Australian Information Security Management Conference, https://doi.org/10.4225/75/58a693deee893.

Amosun, P.A., Ige, O.A., Choo, K.K.R., 2013. Impact of a participatory cybercrime prevention programme on secondary school students' attainment in crime prevention concepts in civic education and social studies. Educ. Inf. Technol. 20 (3), 505–518. https://doi.org/10.1007/s10639-013-9298-0.

Angulo, J., Ortlieb, M., 2015. "WTH..!?!" Experiences, reactions, and expectations related to online privacy panic situations. Proceedings of the Symposium on Usable Privacy and Security (SOUP). Available at: https://www.usenix.org/conference/soups2015/proceedings/presentation/angulo, Accessed date: 15 March 2018.

Anthopoulos, L.G., 2017. Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick? Springer International Publishinghttps://doi.org/10.1007/978-3-319-57015-0.

Arachchilage, N.A.G., Love, S., Beznosov, K., 2016. Phishing threat avoidance behavior. Comput. Hum. Behav. 60 (C), 185–197. https://doi.org/10.1016/j.chb.2016.02.065. July 2016.

Baek, Y.M., Kim, E.M., Bae, Y., 2014. My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns. Comput. Hum. Behav. 31, 48–56. https://doi.org/10.1016/j.chb.2013.10.010. (Feb. 2014).

Ball, A.L., Ramim, M.M., Levy, Y., 2015. Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. Online J. Appl. Knowl. Manag. 3 (1), 108–207. Available at: http://www.iiakm.org/ojakm/articles/2015/volume3_1/OJAKM_Volume3_1pp180-207.pdf, Accessed date: 20 March 2018.

Bartoli, A., Hernandez-Serrano, J., Sorian, M., Dohler, M., Kountouris, A., Barthel, D., 2011. Security and privacy in your smart city. Proceedings of Barcelona Smart Cities Congress. Available at: http://www.cttc.es/publication/security-and-privacy-in-your-smart-city/, Accessed date: 28 December 2017.

Batty, M., Axhausen, K.W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G., Portugali, Y., 2012. Smart cities of the future. Eur. Phys. J. Spec. Top. 214 (1), 481–518. https://doi.org/10.1140/epjst/e2012-01703-3. (November 2012).

BBC, 2018. Facebook scandal 'hit 87 million users'. Available at: http://www.bbc.com/news/technology-43649018, Accessed date: 18 April 2018.

Bellman, S., Johnson, E.J., Kobrin, S.J., Lohse, G.L., 2004. International differences in information privacy concerns: a global survey of consumers. Inf. Soc. 20, 313–324.

Beltran, V., Skarmeta, A.F., Ruiz, P.M., 2017. An ARM-compliant architecture for user privacy in smart cities: SMARTIE—quality by design in the IoT. Wirel. Commun. Mob. Comput. https://doi.org/10.1155/2017/3859836.

Bergström, A., 2015. Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses. Comput. Hum. Behav. 53, 419–426. https://doi.org/10.1016/j.chb.2015.07.025. (Dec. 2015).

Bertot, J.C., Jaeger, P.T., Hansen, D., 2012. The impact of polices on government social media usage: issues, challenges, and recommendations. Gov. Inf. Q. 29 (1), 30–40. https://doi.org/10.1016/j.giq.2011.04.004.

Bianchini, D., Avila, I., 2014. Smart cities and their smart decisions: ethical considerations. IEEE Technol. Soc. Mag. 33 (1), 33–40. https://doi.org/10.1109/MTS.2014.2301854.

Bird, K., 2017. Keeping people at the centre of smart city initiatives. Available at: https://www.iso.org/news/ref2247.html, Accessed date: 30 March 2018.

Bright, J., Margetts, H., Hale, S., Yasseri, T., 2014. The Use of Social Media for Research and Analysis: A Feasibility Study. Available at: file:///C:/Users/User01/Desktop/use-of-social-media-for-research-and-analysis.pdf (Accessed 28 February 2018).

British Standards Institute (BSI), 2016. Mapping Smart City Standards: Based on a Data Flow Model. Available at: http://www.bsigroup.com/en–GB/smart–cities/smart–-cities–standards–mapping–research–and–modelling/ (Accessed 30 August 2018).

Brown, I., Zukowski, T., 2007. Examining the influence of demographic factors on internet users' information privacy concerns. In: Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, pp. 197–204.

Cavazza, F., 2017. Social Media Landscape 2017. Available at: https://fredcavazza.net/2017/04/19/social-media-landscape-2017/, Accessed date: 25 February 2018.

Cecere, G., Guel, F.L., Soulié, N., 2015. Perceived internet privacy concerns on social networks in Europe. Technol. Forecast. Soc. Chang. 96 (2015). https://doi.org/10.1016/j.techfore.2015.01.021. 277–28.

Cobb, S., 2016. Data privacy and data protection: US law and legislation. Available at: https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacy-legislation-white-paper.pdf, Accessed date: 15 March 2018.

Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P., 2005. Location disclosure to social relations: Why, when, & what people want to share. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '05). ACM, pp. 81–90. https://doi.org/10.1145/1054972.1054985.

Conteh, N.Y., Schmick, P.J., 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int. J. Adv. Comput. Res. 6 (23). http://dx.doi.org/10.19101/IJACR.2016.623006.

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

Dong, C., Jin, H., Knijnenburg, B.P., 2015. Predicting privacy behavior on online social networks. In: AAAI Conference on Weblogs and Social Media (ICWSM), Available at: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10554, Accessed date: 15 March 2018.

Doran, D., Severin, K., Gokhale, S., Dagnino, A., 2014. Social Media Enabled Human Sensing for Smart Cities. AI Communications, pp. 2014. Available at: http://knoesis.wright.edu/sites/default/files/aic14.pdf, Accessed date: 28 December 2017.

EDPS (European Data Protection Supervisor), 2018. The history of the general data protection regulation. Available at. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en, Accessed date: 15 April 2018.

Efstathiades, H., Antoniades, D., Pallis, G., Dikaiakos, M.-D., 2015. Identification of key locations based on online social network activity. In: Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, https://doi.org/10.1145/2808797.2808877.

Elmaghraby, A.S., Losavio, M.M., 2014. Cyber security challenges in smart cities: safety, security and privacy. J. Adv. Res. 5, 491–497. https://doi.org/10.1016/j.jare.2014.02.006.

EU GDPR Portal, 2018. GDPR key changes. Available at. https://www.eugdpr.org/the-regulation.html, Accessed date: 15 April 2018.

Falher, G.L., Gionis, A., Mathioudakis, M., 2015. Where is the Soho of Rome?? Measures and algorithms for finding similar neighborhoods in cities. In Proceeding of the Ninth International AAAI Conference on Web and Social Media. Available at: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10514, Accessed date: 25 February 2018.

Fire, M., Goldschmidt, R., Elovici, Y., 2014. Online social networks: threats and solutions. IEEE Commun. Surv. Tutorials 16 (4), 2019–2036 Fourth Quarter.

Fogel, J., Nehmad, E., 2009. Internet social networking communities: risk taking, trust, and privacy concerns. Comput. Hum. Behav. 25 (1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006.

Furnell, S., 2008. End-user security culture a lesson that will never be learnt? Comput. Fraud Secur. 2008 (4), 6–9. https://doi.org/10.1016/S1361-3723(08)70064-2.

Gangadharbatla, H., 2008. Facebook me: collective self-esteem, need to belong, and internet self-efficacy as predictors of the iGeneration's attitudes toward social networking sites. J. Interact. Advert. 8 (2). https://doi.org/10.1080/15252019.2008.10722138.

Giatsoglou, M., Chatzakou, D., Vakali, A., 2015. User communities evolution in microblogs: a public awareness barometer for real world events. World Wide Web 18, 1269. https://doi.org/10.1007/s11280-014-0301-5.

Giffinger, R., Gudrun, H., 2010. Smart cities ranking: an effective instrument for the positioning of cities? ACE 4 (12), 7–25. (February 2010). http://hdl.handle.net/2099/8550.

Gkatziaki, V., Giatsoglou, M., Chatzakou, D., Vakali, A., 2017. DynamiCITY: revealing city dynamics from citizens social media broadcasts. Inf. Syst. https://doi.org/10.1016/j.is.2017.07.007.

Greenfield, A., 2013. Against the Smart City (The City is Here for You to Use). Do Projects, New York.

Gross, R., Acquisti, A., 2005. Information revelation and privacy in online social networks (The Facebook case). In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES'05), https://doi.org/10.1145/1102199.1102214.

Groth, A., 2018. Facebook's data scandal and Europe's new data privacy rule have massive implications for U.S. entrepreneurs. Available at: https://www.entrepreneur.com/article/311273, Accessed date: 15 April 2018.

Gundecha, P., Barbier, G., Liu, H., 2011. Exploiting vulnerability to secure user privacy on a social networking site. In: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 511–519. https://doi.org/10.1145/2020408.2020489.

Hanna, R., Rohm, A., Crittenden, V.L., 2011. We're all connected: the power of the social media ecosystem. Bus. Horiz. 54 (3), 265–273. https://doi.org/10.1016/j.bushor.2011.01.007.

Hoadley, C.M., Xu, H., Lee, J.-J., Beth, R.M., 2010. Privacy as information access and illusory control: the case of the Facebook news feed privacy outcry. Electron. Commer. Res. Appl. 9 (2010), 50–60. https://doi.org/10.1016/j.elerap.2009.05.001.

Hugl, U., 2011. Reviewing person's value of privacy of online social networking. Internet Res. 21 (4), 384–407. https://doi.org/10.1108/10662241111158290.

Hutchinson, A., 2016. Here's why Twitter is so important, to everyone. Available at: https://www.socialmediatoday.com/social-networks/heres-why-twitter-so-important-everyone, Accessed date: 28 February 2018.
International Standards Organization (ISO), 2015. Smart Community Infrastructures – Principles and Requirements for Performance Metrics. Available at: https://www.iso.org/obp/ui/#iso:std:iso:ts:37151:ed–1:v1:en (Accessed 25 August 2018).
ISO/IEC JTC1 Information Technology, 2015. Smart cities. Available at. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf, Accessed date: 30 March 2018.
ISO/TC 268, 2017. ISO/CD 37122: Sustainable Development in Communities -Indicators for Smart Cities. Available at: https://www.iso.org/standard/69050.html (Accessed Sept. 2018).
ITU-T FG-SSC, 2014. Overview of key performance indicators in smart sustainable cities. Available at. https://www.itu.int/en/itu-t/focusgroups/ssc/documents/approved_deliverables/tr-overview-ssc.docx, Accessed date: 30 March 2018.
Jang-Jaccard, J., Nepal, S., 2014. A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. 80 (5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005.
Jensen, C., Potts, C., Jensen, C., 2005. Privacy practices of internet users: self-reports versus observed behaviour. Int. J. Hum. Comput. Stud. 63, 203–227.
Kantarci, B., Mouftah, H.T., 2014. Trustworthy sensing for public safety in cloud-centric internet of things. IEEE Internet Things J. 1 (4). https://doi.org/10.1109/JIOT.2014.2337886. (Aug. 2014).
Kim, S.K., Park, M.J., Rho, J.J., 2015. Effect of the government's use of social media on the reliability of the government: focus on twitter. Public Manag Rev. 17 (3). https://doi.org/10.1080/14719037.2013.822530.
Kirby, T., 2014. Controversy surrounds England's new NHS database. Lancet 383, 9918. http://www.thelancet.com/journals/lancet/article/PIIS0140-6736(14)60230-0/fulltext.
Kisekka, V., Bagchi-Sen, S., Raghav Rao, H., 2013. Extent of private information disclosure on online social networks: an exploration of Facebook mobile phone users. Comput. Hum. Behav. 29 (2013), 2722–2729. https://doi.org/10.1016/j.chb.2013.07.023.
Kitchin, R., 2014. The real–time city? Big data and smart urbanism. GeoJournal 79 (1), 1–14. https://doi.org/10.1007/s10708–013–9516–8. (February 2014).
Kitchin, R., 2016. The ethics of smart cities and urban science. Phil. Trans. R. Soc. A 374 (2083). https://doi.org/10.1098/rsta.2016.0115.
Knijnenburg, B.P., Kobsa, A., Jin, H., 2013. Dimensionality of information disclosure behavior. Int. J. Hum. Comput. Stud. 71 (12), 1144–1162. https://doi.org/10.1016/j.ijhcs.2013.06.003.
Komninos, N., 2013. Intelligent Cities Innovation, Knowledge Systems and Digital Spaces, 1st Edition. Routledge, London. https://www.taylorfrancis.com/books/9781135159306.
Kuczerawy, A., Coudert, F., 2011. Privacy settings in social networking sites: is it fair? In: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (Eds.), Privacy and Identity Management for Life. Privacy and Identity 2010. IFIP Advances in Information and Communication Technology, vol 352 Springer, Berlin, Heidelberg.
Kumar, K.E., Ahmed, H.A., July 2016. 2016. Estimation of traffic with accuracy through twitter stream analysis. Int. J. Innov. Technol. 04 (08), 1317–1324.
Lederer, S., Mankoff, J., Dey, A.K., 2003. Who wants to know what when? Privacy preference determinants in ubiquitous computing. In: CHI '03 Extended Abstracts on Human Factors in Computing Systems (CHI EA '03). DOI, ACM, pp. 724–725. https://doi.org/10.1145/765891.765952.
Lee, J., Lee, H., 2014. Developing and validating a citizen-centric typology for smart city services. Gov. Inf. Q. 31, s93–s105. https://doi.org/10.1016/j.giq.2014.01.010.
Levy, Y., Ramim, M.M., 2009. Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM). Interdiscip. J E-Learning objects 5, 318–319. Available at: http://nsuworks.nova.edu/gscis_facarticles/31, Accessed date: 30 January 2018.
Li, Y., Li, Y., Yan, Q., Deng, R.H., 2015. Privacy leakage analysis in online social networks. Comput. Secur. 49, 239–254. https://doi.org/10.1016/j.cose.2014.10.012.
Luo, R., Brody, R., Seazzu, A., Burd, S., 2011. Social engineering: the neglected human factor for information security management. Inf. Resour. Manag. J. 24 (3), 1–8. https://doi.org/10.4018/irmj.2011070101. (July 2011).
Luo, F., Cao, G., Mulligan, K., Li, X., 2016. Explore spatiotemporal and demographic characteristics of human mobility via Twitter: a case study of Chicago. Appl. Geogr. 70, 11–25. https://doi.org/10.1016/j.apgeog.2016.03.001. (May 2016).
Macenaite, M., Kosta, E., 2017. Consent for processing children's personal data in the EU: following in US footsteps? Inf. Commun. Technol. Law 26 (2), 146–197. https://doi.org/10.1080/13600834.2017.1321096.
Madejski, M., Johnson, M., Bellovin, S.M., 2011. The Failure of Online Social Network Privacy Settings. Columbia University Academic Commonshttps://doi.org/10.7916/D8NG4ZJ1.
Marinaro, L., 2016. Building smart cities starts with smart people. Available at: https://readwrite.com/2016/07/05/building-smart-cities-starts-with-smart-people/, Accessed date: 30 March 2018.
Marr, B., 2017. 17 'Internet Of Things' facts everyone should read. Available at: https://www.forbes.com/sites/bernardmarr/2015/10/27/17-mind-blowing-internet-of-things-facts-everyone-should-read/#63c4bda63505, Accessed date: 25 February 2018.
Martinez-Balleste, A., Pérez-Martínez, P.A., Solanas, A., 2013. The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Commun. Mag. 51 (6), 136–141. https://doi.org/10.1109/MCOM.2013.6525606. (June 2013).
Mazhelis, O., Hämäläinen, A., Asp, T., Tyrväinen, P., 2016. Towards enabling privacy preserving smart city apps. In: Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2). IEEE. https://doi.org/10.1109/ISC2.2016.7580755.
McGrath, F., 2017. Top 10 Reasons for Using Social Media. GlobalWebIndex Available at: http://blog.globalwebindex.net/chart-of-the-day/social-media/, Accessed date: 30 January 2018.
Minkus, T., Liu, K., Ross, K.W., 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), pp. 776–786. https://doi.org/10.1145/2736277.2741124.
Moustaka, V., Vakali, A., Anthopoulos, L.G., 2017. CityDNA: smart city dimensions' correlations for identifying urban profile. In: Proceedings of the 26th International World Wide Web Conference (WWW2017). ACM. https://doi.org/10.1145/3041021.3054714.
Moustaka, V., Vakali, A., Anthopoulos, L.G., 2018a. A systematic review for smart city data analytics. ACM Comput. Surv. https://doi.org/10.1145/3239566.
Moustaka, V., Theodosiou, Z., Vakali, A., Kounoudes, A., 2018b. Smart cities at risk!: privacy and security threats borderlines from social networking in cities. In: 2018 Web Conference Companion (WWW' 18 Companion). ACM. https://doi.org/10.1145/3184558.3191516.
Nam, T., Pardo, T.A., 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. https://doi.org/10.1145/2037556.2037602.
Netter, M., Riesner, M., Weber, M., Pernul, G., 2013. Privacy settings in online social networks - preferences, perception, and reality. In: Proceedings of the 2013 46th Hawaii International Conference on System Sciences (HICSS). IEEE. https://doi.org/10.1109/HICSS.2013.455.
Nokia, 2016. Machina Research Smart City Playbook. Available at: https://pages.nokia.com/2170.What.Are.Cities.Doing.to.Be.Smart.html, Accessed date: 25 February 2018.
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. J. Consum. Aff. 41 (1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x.
Notar, C.E., Padgett, S., Roden, J., 2013. Cyberbullying: resources for intervention and prevention universal. J. Educ. Res. 1 (3), 133–145. https://doi.org/10.13189/ujer.2013.010301.
Nuaimi, E.A., Neyadi, H.A., Mohamed, N., Al-Jaroodi, J., 2015. Applications of big data to smart cities. J. Internet Serv. Appl. 6 (25). https://doi.org/10.1186/s13174-015-0041-5.
O'Connor, N., 2018. Reforming the U.S. approach to data protection and privacy. Available at: https://www.cfr.org/report/reforming-us-approach-data-protection, Accessed date: 15 April 2018.
O'Neil, D., 2001. Analysis of internet users' level of online privacy concerns. Soc. Sci. Comput. Rev. 19, 17–31. https://doi.org/10.1177/089443930101900103.
Parsons, M., 2017. Asia Pacific data protection and cyber security guide 2017. Available at: https://www.hlmediacomms.com/2017/04/11/6461/, Accessed date: 15 April 2018.
Patsakis, C., Zigomitros, A., Papageorgiou, A., Solanas, A., 2014. Privacy and security for multimedia content shared on OSNs: issues and countermeasures. Comput. J. 58 (4), 518–535. https://doi.org/10.1093/comjnl/bxu066.
Rauniar, R., Rawski, G., Yang, J., Johnson, B., 2014. Technology acceptance model (TAM) and social media usage: an empirical study on Facebook. J. Enterp. Inf. Manag. 27 (1), 6–30. https://doi.org/10.1108/JEIM-04-2012-0011.
Rizzo, G., Meo, R., Pensa, R.G., Falcone, G., Troncy, R., 2016. Shaping City Neighborhoods Leveraging Crowd Sensor. Inf. Syst. https://doi.org/10.1016/j.engappai.2012.05.005. (July 2016).
Robinson, N., Graux, H., Botterman, M., Valeri, L., 2009. Review of the European Data Protection Directive. RAND Corporation, Santa Monica, CA Available at: https://www.rand.org/pubs/technical_reports/TR710.html, Accessed date: 15 April 2018.
Saridakis, G., Benson, V., Enzingeard, J.N., Tennakoon, H., 2016. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technol. Forecast. Soc. Chang. 102, 320–330. https://doi.org/10.1016/j.techfore.2015.08.012.
SCC Europe Staff, 2018. How the EU's GDPR will be a game changer for cities using open data. Available at: https://eu.smartcitiescouncil.com/article/how-eus-gdpr-will-be-game-changer-cities-using-open-data, Accessed date: 15 April 2018.
Schivinski, B., Dabrowski, D., 2016. The effect of social media communication on consumer perceptions of brands. J. Mark. Commun. 22 (2). https://doi.org/10.1080/13527266.2013.871323.
Sheehan, K.B., 2002. Toward a typology of internet users and online privacy concerns. Inf. Soc. 18, 21–32. https://doi.org/10.1080/01972240252818207.
Shillair, R., Cotton, S.-R., Tsai, H.-Y.-S., Alhabash, S., LaRose, R., Rifon, N.-J., 2015. Online safety begins with you and me: convincing internet users to protect themselves. Comput. Hum. Behav. 48, 199–207. https://doi.org/10.1016/j.chb.2015.01.046.
Shin, D.H., 2010. The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. Interact. Comput. 22 (2010), 428–438. https://doi.org/10.1016/j.intcom.2010.05.001.
Smart Trikala, 2018. Available at: https://trikalacity.gr/en/smart-trikala/, Accessed date: 3 September 2018.
Smith, K., 2016. Marketing: 96 amazing social media statistics and facts. Brandwatch blog. Available at. https://www.brandwatch.com/blog/96-amazing-social-media-statistics-and-facts-for-2016/, Accessed date: 30 January 2018.
Solomon, M.G., Sunderam, V., Xiong, L., Li, M., 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. https://doi.org/10.1109/ISC2.2016.7580757.
Solove, D.J., 2006. A taxonomy of privacy. Univ. Pa. Law Rev. 154, 477–560. https://doi.org/10.2307/40041279.

Statista, 2018. Number of social media users worldwide from 2010 to 2021 (in billions). Available at. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/, Accessed date: 23 January 2018.
Stross, R., 2009. When Everyone's a Friend, is Anything Private? N.Y. TIMES March 7, 2009, Available at. http://www.nytimes.com/2009/03/08/business/08digi.html, Accessed date: 15 March 2018.
Sundar, S.S., Marathe, S.S., 2010. Personalization versus customization: the importance of agency, privacy, and power usage. Hum. Commun. Res. 36 (3), 298–322. https://doi.org/10.1111/j.1468-2958.2010.01377.x.
The Guardian, 2018. Inside Greece's first smart city: 'Now you don't need to know a politician to get something done. Available at: https://www.theguardian.com/cities/2018/sep/04/trikala-greece-first-smart-city-dont-need-to-know-a-politician-to-get-something-done, Accessed date: 5 September 2018.
Tierney, M., Spiro, I., Bregler, C., Subramanian, L., 2013. Cryptagram: Photo privacy for online social media. In: Proceedings of the 1st ACM Conference on Online Social Networks (COSN'13). ACM, New York, NY, USA, pp. 75–88.
Townsend, A., 2013. Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. W.W. Norton & Co., New York.
Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., Sirivianos, M., 2016. Cyber Security risks for minors: a taxonomy and a software architecture. In: Proceedings of 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP'16). IEEE. https://doi.org/10.1109/SMAP.2016.7753391.
Vakali, A., Angelis, L., Giatsoglou, M., 2013. Sensors talk and humans sense towards a reciprocal collective awareness smart city framework. In: Proceedings of the 2013 IEEE International Communications Workshops (ICC' 13). IEEE, pp. 189–193. https://doi.org/10.1109/ICCW.2013.6649226.
Valerio, P., 2018. Europe's GDPR slaps data collected by cities. Available at: https://citiesofthefuture.eu/europes-gdpr-slaps-data-collected-by-cities-e9118fc648ab, Accessed date: 15 April 2018.
Yang, C., Xiao, M., Ding, X., Tian, W., Zhai, Y., Chen, J., Liu, L., Ye, X., 2018. Exploring human mobility patterns using geo-tagged social media data at the group level. J. Spat. Sci. https://doi.org/10.1080/14498596.2017.1421487.
Yao, M.Z., Rice, R.E., Wallis, K., 2007. Predicting user concerns about online privacy. J. Am. Soc. Inf. Sci. Technol. 58 (5), 611–762. https://doi.org/10.1002/asi.20530.
Yin, F.S., Liu, M.L., Lin, C.-P., 2015. Forecasting the continuance intention of social networking sites: assessing privacy risk and usefulness of technology. Technol. Forecast. Soc. Chang. 99 (2015), 267–272. https://doi.org/10.1016/j.techfore.2015.07.019.
ZEPHORIA Digital Marketing, 2017. The Top 20 valuable Facebook statistics. Available at: https://zephoria.com/top-15-valuable-facebook-statistics/, Accessed date: 30 January 2018.
Zhang, C., Sun, J., 2010. Privacy and security for online social networks: challenges and opportunities. IEEE Netw. 24 (4). https://doi.org/10.1109/MNET.2010.5510913. (July–August 2010).
Zoonen, L.V., 2016. Privacy concerns in smart cities. Gov. Inf. Q. 33 (3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004. (July 2016).

Vaia Moustaka is a PhD candidate and works as a research associate at the Department of Informatics, Aristotle University. She holds an M.Eng. in Electrical & Computer Engineering from Aristotle University of Thessaloniki, Greece, and a M.A. in Public Relations and Marketing with New Technologies from TEI of Western Macedonia, Greece. Her research interests focus on sentiment and affective analysis, research approaches on data metrics and mining and social network analysis, and data analytics on smart cities.

Zenonas Theodosiou received a Diploma in Electronic & Computer Engineering from Technical University of Crete in 2005 and a PhD in Image Processing from Cyprus University of Technology in 2014. He worked as a research associate at the Artificial Intelligence and Image Analysis laboratory at the Department of Informatics of the Aristotle University of Thessaloniki and at the Department of Communication and Internet Studies of the Cyprus University of Technology. His research interests include automatic image annotation, machine learning and data analytics.

Athena Vakali is a professor, Vice Chair at the Department of Informatics, Aristotle University, where she leads the Laboratory on Data and Web science (Datalab). Her current research interests include big data mining and analytics, Future Internet applications and enablers, online social networks mining, as well as on online sources data management on the cloud. She has co-edited 3 books, co-authored 16 book chapters, published over than 60 papers in refereed journals and over 95 papers in International conferences.

Anastasis Kounoudes received his M.Eng. in Computer Engineering and Informatics from University of Patras, Greece, in 1997 and his PhD in Signal Processing from Imperial College in 2000. During the period 2000–2002 he worked as a postdoctoral research associate at the digital signal processing group of Imperial College and as a consultant and researcher at DERA and Qinetiq for telecommunication contracts. Since January 2004, he was the Chief Technical Officer of SignalGeneriX Ltd. and from 2008 the CEO of the company.

Leonidas G. Anthopoulos is an Associate Professor at the Business School of the TEI of Thessaly. He holds an extensive IT research, planning and Management. At his previous job positions, he was responsible for planning and managing the development of multiple IT projects for the Greek Government and for various Public Organizations. He has authored 1 book, co-edited 4 books, and published more than 80 articles scientific journals, chapter collections and international conferences. His research interests concern, among others, smart city, e-Government, Enterprise Architecture, strategic management, etc.