PROTECTION OF PRIVACY AND PERSONAL DATA IN THE BIG DATA ENVIRONMENT OF SMART CITIES

Ahmet Denker
Department of Electrical & Electronics Engineering, Faculty of Engineering and Natural Sciences,
Istanbul Bilgi University, 34060 Eyüpsultan, Istanbul, Turkey
ahmet.denker@bilgi.edu.tr

ISPRS TC IV (WG IV-1)

KEY WORDS: Smart Cities, Smartphones, Big Data, The Cloud, Privacy, Personal Data.

ABSTRACT:

The project of smart cities has emerged as a response to the challenges of twenty-first- century urbanization. Solutions to the fundamental conundrum of cities revolving around efficiency, convenience and security keep being sought by leveraging technology. Notwithstanding all the conveniences furnished by a smart city to all the citizens, privacy of a citizen is intertwined with the benefits of a smart city. The development processes which overlook privacy and security issues have left many of the smart city applications vulnerable to non-conventional security threats and susceptible to numerous privacy and personal data spillage risks. Among the challenges the smart city initiatives encounter, the emergence of the smartphone-big data-the cloud coalescence is perhaps the greatest, from the viewpoint of privacy and personal data protection. As our cities are getting digitalized, information comprising citizens' behavior, choices, and mobility, as well as their personal assets are shared over smartphone-big data-the cloud coalescences, thereby expanding cyber-threat surface and creating different security concerns. This coalescence refers to the practices of creating and analyzing vast sets of data, which comprise personal information. In this paper, the protection of privacy and personal data issues in the big data environment of smart cities are viewed through bifocal lenses, focusing on social and technical aspects. The protection of personal data and privacy in smart city enterprises is treated as a socio-technological operation where various actors and factors undertake different tasks. The article concludes by calling for novel developments, conceptual and practical changes both in technological and social realms.

1. INTRODUCTION

Smart cities' appeal is conspicuous and undeniable; services and conveniences they offer are neither to be rejected nor ignored (Caragliu, 2011). They may provide solutions to some of the severest urban problems including but not limited to energy conservation, sustainable clean environment, monitoring health, optimizing resources, maintaining public safety, etc. (Kitchin, 2014). That is why, the future of smart cities as a project is important. However, while technology supremacism drives cities towards getting smarter, this project will be derailed if it fails to get the privacy issue right. What is meant by the privacy issue, here, is the vulnerability of data to either intentional threats or unintentional breaches because of technical failures or regulatory inadequacies. Smart cities are critically dependent on three technological building-blocks: smartphones; big data; and the cloud. Cities are the most sophisticated structures ever created by men, and interlacing them with similarly complicated structures, reliant on smartphones, big data, and the cloud makes them even more complex and extremely vulnerable to security threats such as cyber-attacks and spillage of personal data (Townsend, 2013). Privacy concerns primarily stem from the vulnerability of the combination of above-mentioned three building-blocks and their prevalent applications. A key issue of concern and worry is the defenselessness of the vast amount of private data (big data) which smart cities garner from ineludible public interactions (smartphones), and storage of that data (the cloud). Privacy and security of this data must be ensured not only as a fundamental right of the citizens, but also as a prerequisite to keeping the faith, trust, and participation of city societies in the future of smart cities. Quite a number of damaging stories circulate which revolve about the privacy and private data. They create skepticism and anxiety concerning the cities and citizens and backlash against smart city projects. This causes technology to be perceived, either rationally or irrationally, as inimical to privacy (Eckhoff, 2018). If we lose faith in the innovative technology, and the way it is deployed in our smartphones and smart cities, social media, home, and vehicles then the backlash may be even more severe - we may see reservation in participating for smart cities, as we have seen resistance to Covid-19 vaccination, especially by the young. If a substantial number of users in smart cities deny, for instance, to be involved with services delivered through smart devices or cloud computing, a digitally dispossessed or marginalized underclass who are unable to access services of the smart cities may be created. This is a foreboding apprehension which needs to be treated by paying attention to privacy and private data protection. In this article, the problem of processing and protecting personal data, which is increasingly prominent in smart city projects, is discussed as a socio-technological process where various actors and different factors undertake prominent tasks. The smart city will still be negatively affected as a project if it fails to answer concerns of privacy; and for the time being this failure is not unlikely. Weaknesses in smartphones-big data-the cloud ensemble manifests itself likely to risk personal privacy of residents and guests of the smart city. Moreover, both technology and regulation together with the actors of the smart city have so far failed to combat with this threat effectively.

2. SMART CITY AND ITS BUILDING BLOCKS

2.1 Smart City

Smart city is a pathbreaking term for a technology-driven city of the future which aims to improve the lives of its dwellers by leveraging high technology. Smart cities are supposed to be increasingly proactive and more responsive to the needs of the residents. These goals are achieved, theoretically, by operating the city on a networked, knowledge-based system. In this ever-increasing competitive environment, security and privacy aspects are often treated as afterthoughts. The development processes which under-implement privacy and security issues have left many of these smart city applications susceptible to non-conventional cyber- threats. Establishing secure smart city services is contingent on the grasp of different cybersecurity features in social and technological branches. Consequently, the efforts in cybersecurity and data privacy in smart cities should be ongoing in two parallel and complementary paths. The first path consists of investigating and identifying various actors and factors and conjoining them with new policies and roles. The second path involves the deployment of technical tools to meet the personal data protection and privacy needs of smart cities. It would be a mistake to assume that the security and privacy issues of smart cities can be resolved by focusing on one of these paths and neglecting the other. Consequentially, it is compelling to view personal data protection and privacy issues of smart cities through bifocal lenses. Smart cities are places where the digital rules bend and blend, but also clash, with the realities of the real world.

2.2 Smartphones

A smart phone is the most outrageous and ubiquitous electronic appliance in stowing and disseminating privacy data. Over the past 20 years, the smartphone has gone from luxury to necessity. While myriad of city functions become accessible to citizens through smartphones, they are also potential information security hazards in smart cities. Highly capable smartphones, in particular, those based on iOS and Android are widely adopted as handheld personal computers (PC's) and personal digital assistants (PDA's). The unprecedented proliferation of smart phones has triggered an overheating race in introducing novel and pathbreaking products for smart city initiatives. However, plans for using smart phones in networked smart cities encounter challenges if they fail to account for data security and privacy issues. The more we have smartphone activities with unskilled users the wider the surface of attack gets. Smartphone users are the weakest link in cyber security of smart cities. Users are mostly individuals without security shrewdness, and their privacy and personal data are vulnerable to increasingly personalized and directed attacks. Configuring how our privacy will be guarded and our personal data will continue to be safe in this enhanced attack surface of smart city-smart phone doublet is a hard task This, not only poses a challenge in and of itself but also has the potential of growing to monstrous scales.

2.3 Big Data

Big data, like smart cities, is a catchall term which has come to use because of transitioning from the "data scarcity" of the past to the "data deluge" of the present. Reduction in the storage cost and processing time of data, improvements in data analysis algorithms, made it possible to store and mine incredibly vast pools of data created by smartphones, etc. The volume of data which can be generated even by a small number of smartphones is astonishing. Smart cities and smartphones are both producers and consumers of big data. Big data, almost invariably involves personal data, we all know that smartphones allow inferences related to private information about their users from stress levels to daily exercises and activities. A specific concern revolves around the potential for repurposing of big data, for objectives other than the original purposes (Ursic, 2018).

2.4 The Cloud

The private data is collected by smart cities mainly through inevitable interactions over smartphones and stored in the cloud. Cloud provides huge advantages in resources and services to users through server networks and service providers. Provisions such as infrastructure, data storage, and purpose-built software are all made actively attainable. However, the prevalent use of clouds for getting and using data from smartphones and applications raises worrisome issues and concerns pertaining to personal data protection and privacy. A key issue is the degree to which smart cities amass personal data. The privatization of ownership of both cloud and data raises question marks concerning the repurposing of "big data" received from the cloud in smart cities. Consequently, smartphone- big data - the cloud coalescence manifests itself as a potential compromise to personal privacy of smart city residents and guests. This makes the mechanism of giving an unequivocal consent to the use of private data by its owner a central issue.

2.5 The Architecture of Smartphones-Big Data-The Cloud Coalescence

Figure 1 displays the smart city-smartphone coalescence system structure. All remote smartphone users (RSU's) will produce their data, such as asset data, home data, mobility data, etc. Data is collected from all RSU's and stored in the cloud. It is conveyed to the Smart City Operation Center (SCOC) through internet.

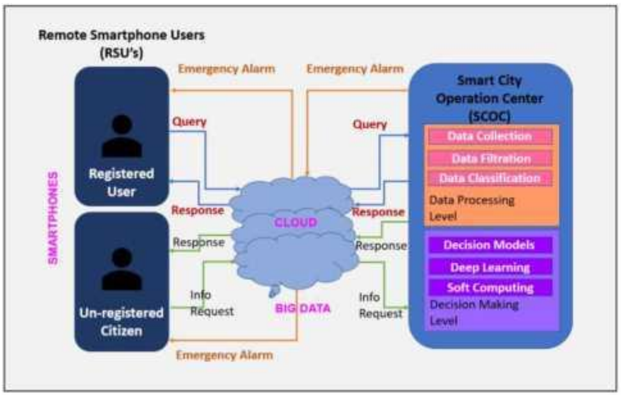

Figure 1. Smart cities have three technological building-blocks: smartphones; big data; and the cloud

SCOC is the brain of the system furnished with a heavy-duty system with parallel processing capabilities. All functions including data collection, processing, and decision making are overlooked here. It is equipped with numerous servers at separate levels. At the level of data processing, all the incoming data is accumulated and stored in data servers. The filtration server filters out and discards all the unnecessary and redundant metadata. Classification of the incoming data from various RSU's is conducted by the classification server according to the message type and the identifier. The decision-making level is empowered with various developed algorithms using decision models, deep learning, image recognition and soft computing. Outside city authorities registered with the system, there exist two types of users who are getting access to the Smart City System. They may be recognized users (the public) who have been registered with the system through a pre-determined procedure, or unregistered users who can indirectly deal with Smart City System to get information from it as guests.

Registered users can make queries in the system, such as asking for the closest hospital, the quickest path to a particular address, free car parking, etc. In addition, if there is any accident or traffic blockage, the system communicates emergency information and alerts to the registered users.

3. SECURITY OF PERSONAL DATA

It is necessary to underline why the security of personal data and protection of privacy is a matter of concern in smart cities. Regardless of all the services and amenities offered by smart cities to common citizens, the legal and technical facets of an individual's privacy are interlaced with the benefits of a smart city (Meijer, 2015). The vast amount of information which is collected through inevitable city operations contain significant amount of sensitive data pertained to the city and the citizens themselves. If all the people information comprising, their behavior, choices, lifestyles, and mobility, in addition to their personal valuables are exposed over the web with inadequate security measures, the result will be a serious overall security threat to the citizens and the city. If this data is compromised by cyber hackers or through repurposing, then the consequences would have harmful repercussions on the citizens and the city overall. Starting from smartphones, any security vulnerability may lead to criminal cases where hackers can have access to the personal assets. Hackers with malicious aims can steal ID and hook the bank accounts information, get hold of address information and data about the people living in the address, as well as vehicular information. Adversaries can carry out any offence based on that information, e.g., with transportation and mobility data, they can track citizens and the autos themselves, and plan criminal activities. They might misguide and manipulate the citizens by communicating false /fabricated information with economic or political motifs. What's more, the attackers can infiltrate into the information of assets of the smart city, itself. In worse cases, with insecure smartphone uses on the internet, a city can be defenseless to cataclysmic criminal acts.

Smart city projects tend to be realized by public-private partnership (PPP), a public agency utilizes the specific tenets and assets of a private-sector entity for the delivery of the smart city services. The Intelligence Operations Center in Rio de Janeiro, which was built by IBM for the 2014 World Cup and 2016 Olympic Games, can be shown as a successful example of PPP, (Edwards, 2016). As has already been stated above, smart cities generate, process, and consume huge amounts of data (big data) of city dwellers and visitors, and PPP applications such as IBM-Rio de Janeiro partnership raise the question of who owns the big data. Contrary to expectations of the citizens and visitors who assume city governments will own and control the big data, it is very likely that in a PPP built smart city data ends up, at least partially or non-exclusively, in private control. What the private-sector entity does with the information it collects is a problematic issue and source of uncertainty and worry for both dwellers and the cities. A citizen's detailed life and behavior patterns can be detected through " data analytics" on information caught in a big data environment.

Big data is fundamentally incompatible with the principle that private data must be gathered for definitive, declared, and legal purposes and not further utilized in any way incompatible with those purposes. Such challenges pertinent to big data require research and innovative thinking on how key data protection principles are implemented in big data applications. They comprise a number of grounds encompassing the consent of the owner of the data. Personal data protection and privacy require that data protection be implanted within the entire life cycle of the smart city technologies. This should incorporate all stages from the launching step, right through to their delivery, processing, and disposal stage.

4. RELATED ACTORS AND FACTORS OF THE SMART CITY

4.1 The Actors

In the reality of smart cities, different actors (for example, different social groups) come together in a complex web of connections and interdependencies due to differences in their interests and understandings. Different actors have radically different interpretations of personal data protection and privacy in the applications of smart cities. Diverse solution preferences arise from these different interpretations.

In determining the relevant actor groups, we can act on the following question: For whom does the protection of personal data have a resembling implication in smart cities? According to the answer to this question, we can divide the actors into three groups: a) Smart city administrators; b) Technology Vendors; c) Citizens.

4.1.1 Smart City Administrators

Regardless of their individual preferences regarding smart city applications, their interpretations arising from their responsibilities and administrative positions will be similar. The problem for them is to find a legal basis for such an undertaking, along with the selection of an appropriate technology, within a certain smart city initiative. Considering how the need for data collection can be met within the framework of accountability, they will consider technological solutions that fall within the limits set by laws and regulations. At the choice stage, the problem for them is balancing the protection of personal data against the public interests of the city such as security, fluent traffic, and crowd monitoring. In their preferences, 'legal framing' is expected to take precedence over 'economic framing'.

4.1.2 Smart City Technology Vendors

The smart city initiative means opening new business opportunities for companies. As mentioned above, the concept of "smart city" is based on the motivation of co-creation and teamwork between city governments, companies, and citizens. As a result, new business models emerge. Undoubtedly, for companies, these new business models manifest as technology-oriented projects. The dynamics and initiatives related to the smart city phenomenon cover many areas (education, health, traffic, energy, etc.), and it is necessary to purchase products and services from many sub-industry fields to successfully develop smart city projects. Another requirement is that companies become part of networks dedicated to such activities so that they have a broad knowledge of smart city initiatives, share best practices, and pinpoint prospective business occasions. Chambers of commerce also have a role to play in promoting this new business area, informing, and disseminating the new way of cooperation, working, and doing business. Companies can also inspire their end users, their customers, to initiate smart city projects in the urban area. Companies for this purpose should take the initiative to inform city governments about current or potential product or service tenders for a smarter city. This way, city managers will be able to learn about projects, products and services that can be ventured jointly with other players in the field of smart cities. Public funds, and particularly local funds, are getting more limited and competitive. Cities' financial capabilities and priorities cannot suffice to finance all smart city projects. In this context, private sector can participate in the smart city initiatives by promoting or proposing projects based on creative financing models. New types of teamwork can be imagined with financial institutions or partners to finance smart city projects. In fact, models in which companies will play a major role in financing and executing these projects can be envisioned. Allied to the growing renown of the smart city phenomenon, it is worthy of consideration that each company, depending on its size, creates a team within its own organization that will produce projects for the problems of the cities of tomorrow.

4.1.3 Citizens

Citizens are in the center of smart city initiatives as a 'related social group', they may view the smart city initiative as a case for them to be monitored and tracked and may be curious or even worried about whether it is necessary. However, if adequate explanation is given) they may also accept the rationale for this, and even expect the benefits to return to them in the form of improved services. The question for them is how to achieve these benefits while giving their information to the public in the least amount and with anonymity. Another issue of concern may be whether data collected for public purposes will fall into the hands of private sector actors for revenue generation purposes. A project can lose acceptance and support, say, if citizens perceive the chosen international company might collect and store their personal data overseas, this would look harmful to them, from the security perspective. However, citizens have often diminished role, and their participation as a central actor needs to be strengthened.

4.2 The Factors

4.2.1 Technology

In the introduction, we argued that the protection of personal data and privacy in smart city enterprises is a socio-technological process where diverse actors and different factors play a variety of roles. Above we tried to define social actors, here the technology leg will be considered as a factor. The arrow points both ways: technology can be influenced by personal data protection requirements as much as personal data protection can be influenced by technology. The success of the smart city initiative, as well as the processing and protection of personal data, depend on technology. Technology is provided by external sources. A medium-sized city, often, lacks the financial resources to afford developing its own technological systems. Outsourcing is the only viable option for most cities, as hardware and software are too challenging to develop, apply, and maintain. These cities can only afford to work with systems proposed and run by third-party vendors. This method is a widespread practice in smart city applications as it decreases expenses, labor, and technological perils. Often such systems are procured as a package which combines diverse functions, as well as software with various data processing capabilities. However, this can cause friction when the administration demands changes to ensure compliance with new regulations by emphasizing privacy and the protection of personal data. The concept of privacy and data protection in the smart city is a comparatively new and sensitive phenomenon and it can be difficult to estimate how costly it is to make the necessary technological changes due to the novelty of the situation. The old contracts did not contain explicit provisions regarding the ownership, access or use of data. Administration may face unforeseen practical complications when contemplating changing vendors, system architectures or contractual agreements, or at least considering precisely by whom the personal data is accessed and controlled.

The result is known in the literature as 'vendor deadlock' for city governments. Also, while contractual arrangements carry the risk of causing vendor lock in, technological deadlock is likely to be significant. In such cases, the city may feel compelled to stick with the same supplier for practical causes such as lack of skill, budget, and time. While new regulations are becoming more commonplace, as technology stabilizes, technology implementation and change becomes precipitously difficult to realize. However, data protection practices will become evident with new technological solutions, and it will be difficult to resist. But we are not that advanced yet.

5. REGULATION OF PRIVATE DATA PROTECTION IN THE EU AND ROLES OF THE ACTORS

Some survey reports echoed the public awareness of privacy issues (Smart-city-meter, 2019). Citizens in European cities have become increasingly aware that a smart city often entails a certain trade-off in terms of privacy. They rightly view this with some discomfort and skepticism. European citizens are more willing to provide data for smart city applications if their privacy is less affected. The results also reveal that citizens want to know for what purposes their data are being used. They are very sensitive and unwilling to accept intrusive initiatives, such as data collection by surveillance cameras which are capable of face recognition.

In recognition of the sensitivity of personal data protection, we will look at the roles and responsibilities of all actors of the smart city. In other words, smart city initiatives should be driven more accountable from the vista of citizens' right to data protection. In smart cities, say, capturing various types of behavior are necessary to find new solutions for increased mobility and livability. However, citizens are more inclined to consent to the use of private data for these issues if they are managed by the government rather than private organizations. Many actors (stakeholders) are involved in smart city projects: citizens, city authorities, technology vendors and citizens. These different stakeholders have also had different views on how the compilation, processing and protection of the data collected in smart city projects. Particularly when this data is personal, the responsibilities for its use and protection are delineated in the General Data Protection Regulation (GDPR) of the European Union (Bieker, 2016).

The most prominent roles and responsibilities of the actors within the framework drawn by the GDPR regarding the protection of personal data in smart city projects, can be listed as:

a) Controllers and processors of data; b) Digital literacy of citizens and city authorities; c) Use and processing of private data; d) Power nonequivalences between public sector organizations and private companies; e) The responsibility of city authorities; g) Sharing and re-using private data.

5.1 Controllers and Processors of Data

In many data processing activities, separating the controllers and processors from each other with thick and precise lines, deciding who will be the controller and who will be the data processor, is a difficult problem and this difficult problem is frequently encountered. Often, technology vendors and smart cities need to process data, whether for shared objectives or for their own goals. Therefore, it is also tricky to differentiate between shared controllership and separate controllership situations. The general view is that data collected in the public domain cannot be freely exchanged between partners. In joint procurement cases where more than one municipality has signed a contract with a single vendor, the controllership can be distributed between the parties (joint controllership). In such cases, practical problems may arise, such as the question of who will have the final say. If all parties must do their own security checks, this can lead to inefficiencies. In such cases, the fact that the vendor is faced with demands from different actors can create a bottleneck. Additional risks may arise in terms of personal data when the same data is shared for different data processing activities by several decentralized data processors. It is known that processing activities cannot always be effectively controlled in smart city applications, especially when vendors do not take any responsibility for the personal data they process. Another issue raised regarding the strong position of certain processors is that sometimes monopoly vendors compel their own data processing terms or diminish the options a municipality may have. One possible solution for such situations is to authorize an independent, central agent. This central agent can either control and manage access to all personal data required by public institutions or decide definitively on the distribution of roles. Also, upon request, this institution may decide who will be the controller(s) and who will be the processor(s) for each new data processing activity. City managers can also take on the coordinating role in smart city projects. Another actor involved in smart city projects is the citizen, if citizens have enough information, they can become their own controllers. However, the general view is that although citizens care about personal data, they feel powerless to control what happens to that data. In literature, such a situation of powerlessness to control what is done with their personal data is referred to as ‘privacy resignation' (Draper, 2016).

5.2 Digital Literacy of Citizens and City Authorities

Digital (or data) literacy is the term used to describe skills, knowledge, and awareness in this field. There is a well-established view that city dwellers (data owners) often lack the necessary literacy. However, the protection of personal data is directly dependent on digital literacy. The demand for privacy must be created by the public, when the public demands it, institutions and companies will follow. Public demand depends on people's caring and digital literacy levels. Moreover, citizens are not the only ones who lack the digital literacy, it is also known that there are those who do not have the necessary literacy among those who work as data controllers in public institutions and municipalities. This situation leads to cases where data controllers cannot understand the difficulties or cannot communicate the problems.

5.3 Legal Basis of Private Data Processing

The processing of personal data in smart city projects must be legally based. The issue of legal basis is therefore important. To ensure the legality of a project, data processing needs to have an appropriate legal basis. The consent of the data owner is a tool used as a legal basis, but in the context of the smart city, the question arises whether the consent is given freely or by the compulsion of city life. It should be noted that where data collection takes place in the public domain, consent may not have been given freely, this fact leads us to question how consent can be obtained in the smart city. While describing forced consent, the terms "public space", "renunciation" and "objection" come to mind. The aggrievement of city dwellers can be prevented by informing about data collection. According to another view, the practice of acknowledging individuals is the fulfillment of a transparency requirement rather than obtaining real consent. In general, there are searches on if and how consent can be implemented effectively, and what alternative legal means can be employed instead of consent, such as legitimate public interest.

5.4 Power Nonequivalence Between Private Companies and Public Sector Organizations

Power nonequivalence between private companies and public sector organizations prevent data controllers from fulfilling their roles and responsibilities. Vendors, especially larger organizations, may be able to have market power to impose their demands. For example, they may use this power to submit requests regarding their right to process and reuse data, and cities may have no choice but to consent to this. Smart cities can be latched to a particular vendor, for example, when there is only one company for a particular technology, or when changing suppliers is too costly or unattainable. Such a power nonequivalence or market failure also makes it impossible for smart cities to comprehensively govern data usage. One solution that can be suggested in this regard is to pool the power of public institutions by promoting cooperation or competition.

5.5 The Responsibility of City Authorities

We should underline that, to ascertain data protection in the smart city, smart city authorities should see themselves as “data controllers” or “data protectors” and assume the main accountabilities to keep data secure and implement safe data governance. To properly fulfill these roles, smart city staff must have the skills required for effective data control, as stated above (See 4.2). Cities must also prevent third parties from accessing personal data. In addition, care must be taken to assure that data sharing for public purposes is provided only through de-identified and anonymized data.

5.6 Sharing and Re-using Private Data

Sharing and re-use of personal data is a sensitive issue, especially for smart city stakeholders. Data governance policies are necessary to avert unwanted sharing. We must emphasize that data collected in the public domain cannot be readily swapped between private and public partners, as there are privacy and confidentiality requirements. However, when such data is also collected by private companies, it must be available for public use.

6. THE GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR), fully enacted across the EU as of May 2018, provides a basis for international harmonization in the EU (Loideain, 2018). The GDPR was a global milestone for privacy and personal data protection. European data protection law provided a solid foundation for a citizen-centered smart city and made the most significant breakthrough in achieving digital security in smart cities. One of the safeguards that the GDPR brings is that personal data can be collected only for “specific, clear and legitimate” purposes and not further processed in a way that is incompatible with these purposes. According to the GDPR, “Processing of personal data is generally prohibited unless expressly permitted by law or permitted by the data subject.” However, it should be considered that there is a risk of finding ways to erode this assurance with big data and data mining. As many authors point out (Zarsky, 2017), purpose specification does not comply with the realities of big data analyses. Analyzing big data entails methods and processes which neither the data collector nor the data subject reckoned or even visualized at the time of collection (Borne, 2013). In other words, starting from the available data, it is possible to reach to the answers to questions that did not even come to mind while collecting these data. With this in mind, it is difficult to see how the GDPR claim of limitation of purpose could prevail. Second, big data challenges the core GDPR doctrine of transparency of processing. Big data resembles a "black box"; data goes in, output comes out, but how that result is generated is often obscured. The algorithm is invisible to the user, and they also learn and change semi-autonomously; this makes it very difficult to document them, hence impeding the transparency of processing. These prospects that big data and data mining offer have raised new questions about how successful the protection measures tried to be brought with GDPR can be, and satisfactory answers to these questions have not been found yet.

7. CONCLUSION

There is a growing sense of foreboding and sensitivity from citizens as well as IT circles, as a warning of the potential threat of smart cities to personal privacy (Allen, 2016). This sensitivity has further demonstrated the importance of ensuring the privacy of individuals and the protection of their personal data. A key issue we have addressed here is how far smart cities go in collecting private data from inevitable public interactions via smartphones. We have also touched on the storage of this "big data" in the cloud, as another important issue parallel to the personal "big data " flow from smartphones. We have sought an answer to the question of who owns and controls the data produced and processed in such large quantities. This question of who owns and controls big data reflects ongoing concerns and uncertainties regarding the protection of private data.

We have looked at the issue of privacy and data protection, which deserve special and bespoke attention, through a bifocal lens, focusing on two problem areas. First, the smart city's dependence on smartphones - big data - the cloud coalescence, secondly, cloud privatization and "big data" ownership and reuse. We've made the argument that the convergence of smartphones - big data - the cloud poses the biggest threats to personal privacy available. While each of these three building blocks of the smart city has been extensively researched in the privacy literature, merging has not been adequately studied.

The insecurity and susceptibility of smart city systems is primarily due to the absence of credibility of this coalescence. Why is this coalescence insecure? This question has been looked at from technical and social perspectives, including a wide range of issues, from digital literacy deficiency to problems of legacy systems in public and private sector systems. There is an obvious problem with the social leg of the lack of alignment in the interpretation of privacy standards and private data security. As a result, privacy in smart cities remains an enigma.

Finally, economic, and social impacts of the crises such as Covid-19 elevate the demand on smart cities to maximize their efficiency, in ways, that can entail erosion of the rights of privacy and private data protection for the sake of "public good." This is likely to ignite a new debate around the "public good" and "privacy" trade-off.

REFERENCES

Allen, N., 2016. Cybersecurity weaknesses threaten to make smart cities more costly and dangerous than their analog predecessors, London School of Economics, London.

Biker., Friedewald, M., Hansen, M., Obersteller, H.,Rost, M. 2016.'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' , in *Privacy Technologies and Policy, Apf 2016*, vol. 9857, S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, Eds. Cham: Springer Int Publishing Ag, 2016, pp. 21-37.

Borne, K. , 2013. Big Data Small World, TED talk, at https://www.youtube.com/watch?v=Zr02fMBfuRA

Caragliu, A., del Bo, C., Nijkamp, P., 2011. Smart cities in Europe. *Journal of Urban Technology*, 18(2), 65-82.

Draper, 2016. 'From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates', Policy & Internet, 9(2), 232-251. https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.142

Edwards, L., 2016. Privacy, Security and Data Protection in Smart Cities, *European Data Protection Law Review*, Vol. 2, pp. 28-58, DOI:10.2139/SSRN.2711290

Eckhoff, D., Wagner, I., 2018. Privacy in the Smart City Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys & Tutorials*, DOI:10.1109/COMST.2017.2748998

Khatoun, R., Zeadally, S., 2017. Cybersecurity and privacy solutions in smart cities. *IEEE*, 55(3), 51-59.

Kitchin, R., 2014. The real-time city? Big data and smart urbanism, *GeoJournal*, vol. 79, no. 1, pp. 1-14. 2014.

Loideain, N., 2018. 'A Port in the Data-Sharing Storm: The GDPR N and the Internet of Things', *SSRN Electron. J.*

Meijer, A., Bolivar, M. P. R., 2015. Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences*, 0(0),1-17.

Smart-city-meter, 2019 https://www.imeccityofthings.be/en/blog/smart-city-meter-2019

Townsend, A., 2013. *Smart cities: big data, civic hackers, and the quest for a new utopia*. New York, NY: W.W. Norton & Company.

Tsiamoulis, C., 2020. The impact of the principles of GDPR, https://www.semanticscholar.org/paper/The-impact-of-the-principles-of-GDPR-Tsiamoulis/e53c3ac2d3af7fd2c1c56bd1b35a6db134139e03

Ursic, H., 2018. The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution? Business, DOI:10.1007/978-3-662-57646-5_4

Zarsky, T. Z., 2017. Incompatible: The GDPR in the Age of Big Data, Business, The Seton Hall Law Review, Vol. 47, pp. 995-1020.