3D Privacy Framework: The Citizen Value Driven Privacy Framework

Edgard Musafiri Mimo, Troy McDaniel
The Polytechnic School
Arizona State university
Mesa, USA
{emusafir, troy.mcdaniel}@asu.edu

Abstract— **The promises of smart cities continue to overwhelm many people eager to live in them. Simultaneously, many people are still concerned about the increasing privacy risks associated with the core of the promises. The core of smart cities' promises lies in generating and using data to enable urban technologies that provide, to some degree, value-added services and opportunities for both cities and their citizens. The promises of smart cities highlight three interdependent dimensions, namely the information type, purpose, and value that provide the basis of studying and addressing privacy concerns to enable successful smart cities. This paper presents a 3D privacy framework based on three interdependent dimensions that build on existing citizens' privacy models [1] and framework [2] to hypothesize when citizens are likely to accept smart city technologies with privacy concerns, when citizens are more likely to accept trading their privacy for the provided valued services under defined regulations, and when citizens are likely to protest and disregard smart cities technologies altogether. The 3D privacy framework highlights new ways of evaluating how technologies impact citizens' privacy and encourages adopting new ways to lessen citizens' privacy concerns by implementing technology-specific agile regulation based on the metrics of security. Some specific examples of smart city technologies are discussed to illustrate the practicality and usefulness of the proposed 3D privacy framework in the smart cities' space.**

Keywords—Smart cities, Privacy, Framework, Security, Surveillance, Awareness, Consent, Permission, Citizen centered.

I. Introduction

The idea of the realization of smart cities that use data to enable new services or improve existing ones is exciting. Nevertheless, the massive data collection to enable technologies in smart cities still raises countless privacy issues. These issues range from identifying whether the information or data being collected is personal or impersonal to whether the enabled service is provided with or without surveillance. Hence, the value of the enabled services through the deployed technologies in smart cities should be evaluated based on what citizens can tolerate concerning their privacy to enable and allow resilient smart cities. Zoonen [2] introduced a 2D framework model as a tool to help analyze and understand how urban planners should integrate privacy concerns in planning and building efficient and desirable smart cities.

It is important to assess different smart cities technologies to understand what types of data is used, determine whether the data is personal or impersonal, and ultimately control the purpose of the enabled technologies. It is vital to evaluate the purpose of enabling services for citizens through technological solutions to determine whether the services are provided with or without surveillance. The consideration of citizens' sentiment in smart cities is necessary to provide practical solutions that answer to the myriad of privacy concerns among citizens.

The understanding of the value aspect of data and technologies remains a key factor in determining whether technology provides value predominantly to citizens or to both cities and citizens. The same comparison can be applied even further to look at whether the enabled services' value is predominantly for the public sector or both the public and private sector; the producer or both the producer and consumers; and so on. Understanding the actual value of the deployed technologies or systems in smart cities helps to differently address the privacy concerns of both the intentional and unintentional service's surveillance. It is essential to provide better services in such a way that there is an active consideration about the use of personal data enabled services without creating a surveillance state with the deployed technologies. Related works [1][3][4][5] point out that the success of smart cities ultimately depends on their capacity to properly address and respond to questions, concerns, risks and consequences that pertain to the privacy and security issues of citizens and their data regardless of the amazing, enabled technologies.

In this regard, it remains paramount to assess every technology within smart cities in a way that addresses the privacy concerns of citizens. Zoonen [2] urged the need to assess the types of technologies that are deployed in smart cities with emphasis on the collected data and the purpose for data collection. The 2D framework proposed in [2] could potentially benefit from a critical value dimension that ripostes to whether the deployed technologies are valuable to either citizens or cities in ways that validate and justify enabling them within smart cities. This paper proposes a 3D privacy framework that aims to answer citizens' privacy driven questions related to the deployed technologies in view of the actual value that the deployed technologies and systems provide to smart cities and its citizens for enabling resilient privacy aware smart cities [1].

The 3D privacy framework with data, purpose and value dimensions results in eight different quadrants or spaces that a smart city technology or system can be categorized after careful evaluation of its data type, enabled services, and provided value to either the city or its citizens. The provided value can be different forms including monetary benefits, security benefits, health benefits, opportunities, etc. Ultimately, the value of a specific system or technology would converge to a monetary value in view of the investments needed to implement and deploy these technologies. When the value provided by a particular technology or system benefit both citizens and smart cities equivalently, the 2D framework [2] can be used to address privacy concerns based on the data type and the purpose of the technology.

However, when there is an indication of more value being provided to either the citizens or the city by the provided service, there is an opportunity to assess the associated privacy concerns with the 3D privacy framework. The assessment could mean using an agile regulation process to set boundaries on how to deal with the collected data in ways that lessen the privacy concerns of the citizens. The agile regulation process considers the security aspects associated with the technology or system being assessed based on different privacy flags. The agile regulation process determines how to mitigate or lessen the privacy concerns by setting guidelines on how long private data should be kept or when to delete them after the service.

The value driven 3D privacy framework is built on frequent dimensions in research on privacy concerns based on how people perceive specific data as more personal and sensitive than others [2] and how people view privacy concerns differently based on the collected data and the provided benefits they enjoy. For example, many social media users care less about the information they share online if they receive their anticipated response from their followers [2]. The efficacy of the 3D privacy framework highlights the premises of a tradeoff for citizens between the level of forgoing privacy or allowing personal information sharing in exchange of personalized services' value that outweighs the privacy concerns, especially when personal data regulations are set up to lessen the privacy concerns.

II. Related Work

Privacy is a fundamental element that smart cities must address to be citizen centered. Privacy demarcated as the right to be let alone [33] has broaden as a notion over time. It contains many other aspects, such as freedom of thoughts, the right to self-isolate, the ability to control personal information, the right to be free from surveillance, the protection of one's reputation, and the protection from searches and investigations [34]. The prospect of privacy cannot be undermined with the extensive deployment of IoT sensors that increasingly collect personal information from both public and private institutions [35]. The collection of personal data is carried out with or without people's granted permission and awareness [36]. All technology whether it is cryptography, blockchain, biometrics, machine learning, and so on, that requires the collection of personal data, induces at least an associated privacy concern element that must be properly addressed to avoid total technological privacy invasion of citizens.

Consequently, there are many avenues for technology driven privacy issues within smart cities, as they shift their attention to the quantitative collection of data through the deployment of sensors and to the automated computational systems modeling for data analysis that optimize the enabled services for citizens. The privacy concerns are enormous and complex to dissect and resolve with more and more data collection without the proper protection and regulation in place. Privacy remains the indispensable component in generating an effective and justifiable value for citizens [37], and every technology that collects and aggregates citizens' personal data must address its concerns.

Technology driven privacy issues occur throughout the lifespan of the technology from conception to development to deployment and finally through lifetime application and use. In the conception phase of the technology that uses personal data, there is a privacy red flag of people's long-term awareness, consent, and willingness to grant permission [2] for the collection of personal data that enable the technology, which must be addressed. In the development phase, there are many privacy risks that raise concerns [38][39] about data use and protection to ensure that no third party can access, and potentially compromise, personal information without people's consent and permission. In the deployment phase, there are other privacy related issues to be mindful of in terms of data security and data aggregation as hackers can exploit the collected data for other uses without the consent and awareness of individuals [39]. Lastly in the lifetime application and use phase, privacy issues arise from different angles in the aggregation of data and the security of different databases and systems [40] that interact with the collected data with or without individual consent and permission.

The datafication of smart cities information and communication technology infused infrastructures enables the extensive monitoring and steering of city maintenance, mobility, air and water quality, energy usage, visitor movements, neighborhood sentiment, etc. It excavates avenues for privacy and security concerns that necessitate in-depth assessment of smart cities technologies and systems to preserve the provided citizens' value. The applicable technology driven privacy issues within smart cities are discussed further in section IV.

III. 3D privacy framework

The privacy level illustrated in the 3D privacy framework is based on how many of the five privacy dimensions, namely identity privacy, query privacy, location privacy, footprint privacy, and owner privacy [1], are encompassed by the given technology or system. The identity privacy dimension pertains to the releasing of the identity of a user when a user accesses a smart city service. The query privacy dimension pertains to the protection of the privacy of the requests made by users to services. The location privacy dimension pertains to the guarantee that the privacy of the user's physical location is protected. The footprint privacy dimension pertains to the control of information that can be recovered or inferred from microdata sets. The owner privacy dimension deals with the privacy-aware computation of queries from different autonomous entities databases.

The higher the number of privacy dimensions the technology or system violates or flags, the higher the overall privacy level the quadrant possesses. Privacy-enhanced technologies should be judged based on different levels of privacy, and the decision to allow their deployment should rest primarily on the value they provide to both smart cities and citizens, and ultimately on the security measures they employ to fulfil their purpose. This is the essence of the 3D privacy framework as it enables new ways of judging different technologies in the smart cities space and offers avenues to assess future deployable technologies.

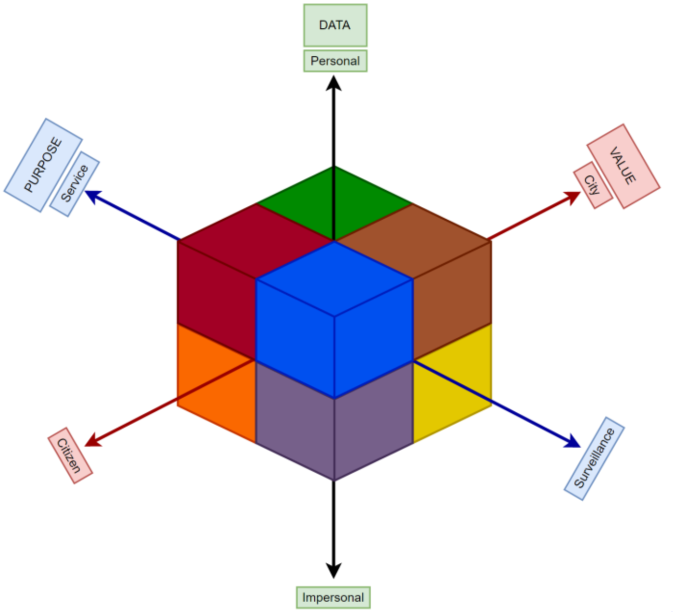

Fig. 1: The figure presents the proposed 3D privacy framework.

The 3D privacy framework is an adaptive technology assessment tool for enabling enhanced citizen's privacy aware technologies based on provided value and services. It facilitates a better approach in analyzing the required regulations that must be put in place to help lessen the privacy concerns of citizens and enables them to adopt more technologies that provide them with true value without jeopardizing their privacy. The crucial distinction of providing services is made resulting in service with surveillance (denotes surveillance) and service without surveillance (denotes service).

It is necessary to mandate strict regulations in lessening the privacy concerns in some quadrants. The mandate may pertain to the deletion of personal data after service completion to avoid further damage or compromise to their personal data used in enabling the service. Knowing the value that the technology provides to citizens might help drive the regulations of how data can be preserved. The 3D privacy framework facilitates privacy discussion and provides a better way of determining whether the technology is valuable and indispensable enough to demand the collection of private or confidential data to realize its purpose and provide its value. The 3D privacy framework as shown in Figure 1 generates eight different quadrants conditioned by the value dimension and dominated by the relationship between the data type and the purpose of the technology or system.

IV. Framework Quadrants

This section discusses the different genres of technology that can potentially fall into each of the eight spaces shown in Figure 2 and highlights at least one example of the current technologies penetrating the smart cities space to address the relevant privacy concerns.

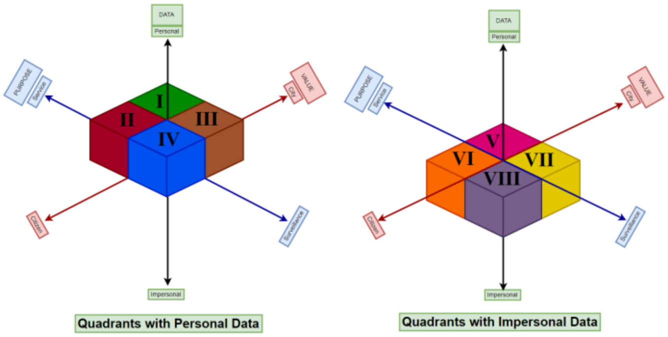

Fig. 2: The figure shows the 3D privacy framework's quadrants based on the data type.

This approach aims to provide a way to weigh the generated privacy concerns against the value that the technology provides to its stakeholders whether it is the citizen or the city, the private sector or public sector, and so forth.

A. *Quadrant I*

The first quadrant revolves around technologies and systems that provide value predominantly to the city by the service they enable using personal data they acquire from citizens. In this space, technologies that provide value to the city by using the personal data of citizens in conjunction with any impersonal data to enable the needed services are concerned. There are many smart technologies and systems that fall into this space like smart mobility technologies that necessitate for the most part a good understanding of citizens' location and movement to better plan for non-congested routes, traffic light durations and more smooth transportation systems including overall traffic control and management systems. Thus, understanding the culture in the city and the behavior of the citizens including their movement is paramount for an efficient and effective smart mobility system because the understanding of how citizens move and their means of movement provide better ways to plan, control and optimize city systems beyond only looking at vehicle movements' patterns.

For example, if the system or application knows where citizens want to travel to at specific moments such as going to work during workdays or to the beach on the weekend, the system and application's algorithm can couple those habits with citizens' location information to plan and align the best routes. Based on citizens' participation, further investment in similar projects may be made to enhance citizens' experiences by improving the city's mobility systems and infrastructure such as road expansions. The privacy level in this quadrant is deemed as high because of the many potential privacy dimensions risks associated with the technologies, and the intention of the potential technologies in this quadrant are not for surveillance. It is apparent that at least three of the five privacy dimensions concerns can be encountered in enabling the needed services for cities. An example of a smart mobility technology and service is discussed in [6][8] to expose the potential privacy dimensions in enabling the services.

In smart mobility technology, there is a high concern for query and location privacy concerns [11] as applications need to identify a point of reference which is coupled with an identity of the user [9] or the mobile device IP address requesting the services. Additionally, there is a footprint privacy concern for the suggestion of common routes and guessing of common places in the request and the delivery of the services. A typical example of smart mobility [9][32] is the sharing and urban mobility service where transport systems are shared between users to optimally provide a multimodal convenient transport system to users. It is evident that the privacy risks associated with the identity, query, location, and footprint [11] privacy is relevant in this space to mandate proper security [10] and regulations.

B. *Quadrant II*

The second quadrant revolves around technologies or systems that provide value predominantly to citizens by the service they enable using personal data they acquire from citizens. In this quadrant, technologies that provide value to citizens by using personal data in conjunction with any impersonal data to enable the needed services should be considered. It is evident to notice a prevalent attribution of smart health technologies and systems whereby citizens are notified of danger zones that could be hazardous for them. Smart health technologies make use of personal information of citizens and more importantly their health history and background including their pedigree to optimally determine and recommend safe measures for individuals to adopt and follow for a better health outcome.

The provided value of technologies and systems in this space is more toward the well-being of citizens even if the cities invest in the infrastructure to support and facilitate the collection and processing of all data to better connect citizens to their health experts. The technologies and systems help and enable health experts to see health related patterns quickly for the patient within his or her immediate environment. It is true that many smart health technology applications would not be possible without the need and use of personal data and information [12]. It is in consideration of the provided value that one can better weigh between the privacy and security concerns and the receivable health benefits. Perhaps when the benefit or value of the technologies and systems dominate, there would be a bigger push in finding ways to regulate technologies and the ownership of the data in a way that facilitate the adoption of similar technologies.

The privacy level in this quadrant is deemed as high because of the potential privacy dimensions risks associated with the technologies, and the purpose of the technologies is not for surveillance. It is evident that at least three of the five privacy dimension concerns can be encountered in enabling the needed services for the cities. A typical example in this space is the e-Health application that provides services to patients like prescription refill by using their previously stored database electronic health record information to facilitate and optimize the services [4].

In the smart health technology application space, there is a high concern for the identity, query and owner [12][13][14] privacy aspects as applications need to identify and authenticate the beneficiary of the service through queries. Queries access the personal information of the beneficiary in the database to ensure there is a substantial match to accurately provide the needed service. There is a need for proper data and information analysis in this space as updating the database information needs to be secured and reliable for proper and accurate servicing of patients [12], otherwise it would be a disaster should the information be compromised in any way, shape or form. Therefore, applications in this space require a proper security mandate and regulations [15] to lessen citizens' privacy concerns [16].

C. *Quadrant III*

The third quadrant revolves around technologies and systems that provide value predominantly to cities with the surveillance systems they enable using personal data acquired from citizens in conjunction with other impersonal data. Smart government security systems are more prevalent and lead in this space to help run and secure smart cities. These systems are built to anticipate security issues within smart cities by possessing and processing critical personal information of citizens [17] and correlate that information to their moves through constant collection of video footage of suspected citizens [18].

In this quadrant, the personal information of citizens is collected, models of artificial intelligence are deployed, machine learning models for face recognition are instituted, and video surveillance systems are operated to realize safer smart cities [19]. These technologies are meant to enable faster information transmission for quicker security responses. Most of the smart technologies in this quadrant may be found in law enforcement [20] because they can greatly benefit from the collection of personal data of citizens [19] to better secure cities in deploying more law enforcement in areas with higher crime history and a higher number of people with crime history. This is the quadrant with the highest level of privacy concerns as more personal information that the government may want might not be easy to obtain from citizens especially when they know that information will facilitate their monitoring and investigation.

The privacy level in this quadrant is deemed highest because of the potential privacy dimensions' risks associated with the technologies coupled with the intent of technologies being for surveillance reasons and pattern recognition. It is evident that at least four of the five privacy dimension concerns are encountered simultaneously in enabling the needed surveillance services for smart cities. Technologies in crime prevention that use video surveillance [2] involve the complete identification of individuals and tracking movements through interconnected surveillance data feeds with other IoT data feeds. In this example, all five privacy dimensions are in play, and the interconnection of these different privacy dimensions results in the highest privacy concerns level that must be addressed and properly regulated. The identity, query, location, footprint and owner privacy concerns [18] [17] cannot be overstated in the acquisition, processing and interpreting the video data feeds to detect and anticipate a specific action and trigger the commanding response [20][31].

D. *Quadrant IV*

The fourth quadrant revolves around technologies and systems that provide value predominantly to citizens by the surveillance systems they enable using personal and confidential data they acquire from citizens and throughout the city. In this quadrant, there is an opportunity for more smart governance technologies, as the systems and applications enable more engagement between citizens and cities to ensure that more value is provided to citizens.

At the same time, the technologies and applications facilitate the connection and communication between both citizens and cities through an iterative process of systems' improvement and bias reduction. The quadrant encompasses technologies that enable citizens in many ways, not limited to only the use of their data. There is value in the provided surveillance services toward citizens in enhancing the security and the overall credibility of the systems and applications. In this space, there is a paradox effect in that there is potential for some citizens to surveil government administrations, agencies and systems to determine how long they take to process the collected data and provide the proposed services [20][31].

The privacy level in this quadrant is deemed highest because of the potential privacy dimensions' risks associated with the technologies in this space, and the aim of the technologies is for surveillance. It is evident that in this quadrant at least four of the five privacy dimension concerns can be encountered in enabling the needed services for citizens. An example of smart governance is discussed in [7][21] to expose the potential privacy dimensions in enabling the surveillance of citizens and gauge their level of acceptance or rejection of a service. Good governance requires the participation of citizens in providing feedback and voicing concerns. There is a need for authentication of citizens [21] and a reliable security in their interaction to facilitate a smart governance service. The identity, query, location, and owner privacy concerns are dominant in this quadrant, and if needed for surveillance, footprint privacy concerns also arise. Hence, there is a greater need for privacy and security issues [20][31] to be addressed in this space together with a set of regulations for the greater good of citizens.

E. *Quadrant V*

The fifth quadrant revolves around technologies and systems that provide value predominantly to cities by the services they enable using impersonal data they acquire throughout the city. In this space, there is a potential for many technologies that provide services and value to a city by ensuring that the city runs optimally and efficiently without generating any privacy violations or concerns. The provided value to cities is brought about by the numerous applications that make use of the myriad of IoT sensors deployed around smart cities. The technologies in this space include smart agriculture, water quality monitoring, air quality monitoring, noise control, heat monitoring, among many other systems.

The type of data collected is impersonal, and IoT sensors are continually developed and deployed to enable data acquisition in real time to optimally facilitate the services provided in smart cities. Many environmental sensors that are currently deployed generate less privacy concerns as they are aimed to only serve the purpose of monitoring changing conditions within the environment to enable citizens to make good decisions as to what they can safely and optimally do in the city.

The privacy level in this quadrant is deemed low since there are hardly any noticeable potential privacy dimensions' risks associated with the technologies in this quadrant as the aim of the technology is to provide services to cities while using impersonal data. It is evident that there is at most one privacy dimension concern, i.e., owner privacy, which is usually irrelevant as most of the data collected in this space are typically open data for environmental services. A good example in this quadrant is air quality monitoring [22] to help manage and control air pollution initiatives within smart cities. Although there may be some security challenges encountered in the collection and analysis of the data, there are, however, minimal privacy concerns with the use of impersonal data for enabling such services in smart cities.

F. *Quadrant VI*

The sixth quadrant revolves around technologies and systems that provide value predominantly to citizens by the service they enable with impersonal data they acquire in the city. In this space, there is potential for many technologies that provide services and value to citizens by ensuring they enjoy their lifestyle and live in a way that is better with technology than without. This is a quadrant where technology is well encouraged as there are no or low potential for privacy concerns, as technologies provide avenues to enable citizens to plan their trips efficiently. In this quadrant, technologies and applications involving weather forecast and environmental informatics are useful and provide valuable information to citizens to enhance safety and planning.

The privacy level in this quadrant is deemed low since there are barely any noticeable potential privacy dimensions' risks associated with the technologies as the aim of the technology is to provide services to citizens or users while using impersonal data. It is obvious that there are usually no privacy concerns involved in this space as it pertains to citizens because none of their data is being collected in enabling the technologies or applications thereof. If there are ever privacy dimension concerns, it will be that of owner privacy which relates to the security and the interactions of the various databases that house data collected by the myriad of deployed sensors in smart cities.

A good example is that of smart home applications that condition the homes to efficiently manage energy by economizing when to dim or turn off lights or adjust the thermostat to enable free cooling [23] and heating depending on the outside conditions. Another example is the weather forecast [24] and conditions to better inform citizens to prepare for their planned activities. All these applications and services are provided without any requirement from citizens to share any personal information. There are some security challenges from the applications providing location specific services; thus, creating the location and query privacy concerns in the collection and analysis of the data. Nevertheless, there is still minimal privacy concerns in enabling the services as the source does not necessitate any use of personal data.

G. Quadrant VII

The seventh quadrant revolves around technologies and systems that provide value predominantly to cities by the surveillance service systems they enable through the use of impersonal data they acquire in the city and from citizens (data such as geographic location). The quadrant privacy concerns arise from the fact that there is surveillance involved in the provided service or in the deployment of the surveillance equipment or sensors that collect impersonal data, but through the aggregation of impersonal data with other data, personal information is acquired. Examples of impersonal data can be location coordinates of a residence which can be aggregated with temperature spikes generated in the home to determine whether an individual is in the home [25] even though the collected data are impersonal.

It is evident that the surveillance services provided to citizens by a city can be questionable because not all individuals are comfortable with being surveilled or targeted in some way. There are specific neighborhoods [26] that can be biasedly targeted, and people living in them would not appreciate revealing any of their personal data during any aggregation process whatsoever. The surveillance example in this quadrant can be that of determining the occupancy of a smart home [27] through the use of aggregated data coupled with some specific appliance power consumption data [29] as the demand and consumption varies with an increasing number of people in the home.

This data aggregation is expanded to virtually indicate the presence of individuals [28] in a home in real time. Household occupancy monitoring [30] through the aggregation of data contributes to privacy concerns as it opens more concerns from citizens as to what personal data are compromised through the footprint and owner privacy concerns. The privacy level in this quadrant is deemed medium because there are potential privacy dimensions' risks associated with the surveillance technologies using impersonal data that is aggregated to reflect and detect sensitive private information. Therefore, there is a need for robust security and regulations to be put in place to lessen citizens' concerns.

H. Quadrant VIII

The eighth quadrant revolves around technologies and applications that provide value predominantly to citizens by the surveillance system enabled using impersonal data acquired in the city. This quadrant becomes swiftly extraneous in the sense that citizens would not be encouraged to go to the extent of using impersonal data to surveil other citizens. Thus, there are not many technologies or systems that would provide the surveilling services and value to citizens in any way that does not violate the privacy rights of other citizens. In this case, the framework does not consider nor recommend anything. However, if there is an opportunity space where some applications can be considered, it may be in parental guidance applications where there could be restrictions to content children are able to access without proper authentication. Nevertheless, it would necessitate some personal data aggregation in providing credentials, locations, and queries to provide a clear value.

V. Framework Relevance

The proposed 3D privacy framework seeks to answer two fundamental questions as it pertains to privacy concerns within smart cities. First, the framework seeks to focus on and assess the various existing technologies that are deployed in smart cities, which use personal data to provide services and value that benefit primarily citizens. In this regard, the framework assesses the surveillance ability of technologies by analyzing the types of data used, and the various data manipulations that are needed to eventually enable valuable services. Thus, it ensures that citizens' personal information is not used for decisions that do not benefit citizens and ensures proper regulations for data deletion after the provided service completion to avoid the use of data for other purposes.

It is evident that citizens are willing to trade some of their personal information for services that are deemed valuable to them, and that can be enabled by using personal information such as in the case of Saudi Arabia [35]. Additionally, the framework considers technologies that provide value to both citizens and cities in the services they enable. In this case, there is a need for personal data storage to build trends and identify patterns as smart cities' needs might vary with time. For example, traffic jam control and reduction due to the mobility of citizens around smart cities require optimization over time to account for specific times citizens prefer to move based on their needs.

These patterns are important to better manage citizens' mobility and migration efficiently to ensure that citizens benefit from not spending excessive amounts of time in traffic under conditions of bad air quality, whereas smart cities benefit from low gas emissions from cars. Thus, the framework aims to determine whether and when citizens can accept technologies that provide value to both them and smart cities by the services they enable even if it means storing personal data.

The research question to consider is whether citizens' concerns of privacy lessen if and only if the value provided by technologies was citizens' only value or the value provided was for both cities and citizens. One can ask a similar question in demanding whether citizens would accept to trade their personal data for technologies that provide value to them only, or to both them and the city through the services they enable. In [35], it is shown that in the case of Saudi Arabia, the tendency of citizens to accept services that provide value to them outweighs some of the privacy concerns involved with using their personal data.

The framework seeks to determine the factors that can potentially affect citizens in choosing provided service value over privacy concerns, and when that is appropriate for the majority of citizens to better assess future technologies and systems. Secondly, the 3D privacy framework seeks to understand the value that technologies using impersonal data provide for both citizens and smart cities and identifies ways technologies using impersonal data can substitute for the technologies that use personal data while providing the same value and services to both citizens and cities. The question is how can technology using impersonal data provide the same services and value as those that are using personal data? This is a pertinent question that would provide a convenient approach to understand how to improve technologies using impersonal data to meet the demand of those using personal data.

TABLE 1: THE 3D PRIVACY FRAMEWORK BASED ON THE PRIVACY ASPECTS IN SMART CITY SERVICES [1]

Data	Purpose	Value	QD	Privacy level	Technology/System
Personal	**Service**	**City**	**I**	**High**	**Smart Mobility**
Personal	**Service**	**Citizen**	**II**	**High**	**Smart Health**
Personal	**Surveillance**	**City**	**III**	**Highest**	**Smart Government, E-Government**
Personal	**Surveillance**	**Citizen**	**IV**	**Highest**	**Smart Governance, citizen's engagement**
Impersonal	**Service**	**City**	**V**	**Low**	**Smart agriculture, water, and air quality monitoring**
Impersonal	**Service**	**Citizen**	**VI**	**Low**	**Smart homes**
Impersonal	**Surveillance**	**City**	**VII**	**Medium**	**Smart grid, smart waste management, smart homes**
Impersonal	**Surveillance**	**Citizen**	**VIII**	**Medium**	**Open data, parental consents apps**

The list of the different quadrants with their associated privacy level within smart cities is given in Table 1. A qualitative experiment will follow up as future work to enhance the literature's findings [35] and help provide insights into the above questions and observations. The privacy related concerns with the 3D privacy framework would normally only apply to the technologies that make use of personal data and provide either the service or the surveillance to citizens or smart cities. It is imperative to consider the quadrants that are associated with the provision of surveillance services while using impersonal data because they are enabled only when the primary impersonal data are aggregated with personal data stored somewhere to provide the surveillance. Otherwise, there would not be any surveillance or privacy concerns to begin with. This 3D privacy framework highlights technologies that provide value to citizens that may be prohibitively expensive to justify investment for deployment. It opens ways to investigate the reasons why these technologies are not being pushed forward and invested in. The privacy concerns arising from the use of personal data for surveillance is detrimental to citizens. The question to answer is whether privacy concerns will lessen if the technologies provide value to the citizens only rather than both citizens and smart cities.

VI. CONCLUSION

The issues surrounding citizens' privacy will continue to be a major decider, enabler, and driver for resilient and successful smart cities. It is imperative to assess the privacy concerns of every technology in smart cities to ensure that they do not violate the privacy rights of citizens while achieving their purpose and providing their intended value. The weight of the five privacy dimensions may differ across context and people; therefore, future research should explore expanding this model with quantitative data from surveys to reflect how citizens of different demography may weigh these privacy dimensions. In doing so, a cumulative quantitative measure of privacy severity level can be used to clearly determine the privacy level range within each proposed 3D privacy framework's quadrant. Such effort may shed light on how to rank the privacy level of each quadrant and reflect what really matters for citizens. The proposed 3D privacy framework provides an avenue to assess both existing technologies and qualify future deployable technologies with the lens of citizens' privacy concerns based on the intended provided value. It is essential to ensure every technology or system being deployed in smart cities is assessed and validated to not violate the privacy rights of its users: the citizens living and using these applications in smart cities. This is an agile and dynamic approach of assessing technologies in smart cities based on what citizens consider as private information to be kept confidential. At the same time, the framework offers an avenue for citizens to weigh the benefit of using personal information to receive services that offer a certain value without necessarily benefiting smart cities with the mandate of agile regulations and policies.

ACKNOWLEDGEMENT

The authors thank Arizona State University and the National Science Foundation for their funding support under Grant No. 1828010.

REFERENCES

[1] A. Martinez-Balleste, P. A. Perez-Martınez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," Communications Magazine, IEEE, vol. 51, no. 6, pp. 136–141, 2013.

[2] Zoonen, Liesbet. (2016). Privacy concerns in smart cities. Government Information Quarterly. 33. 10.1016/j.giq.2016.06.004.

[3] Ijaz, Sidra & Shah, Munam & Khan, Abid & Ahmed, Mansoor. (2016). Smart Cities: A Survey on Security Concerns. International Journal of Advanced Computer Science and Applications. 7. 10.14569/IJACSA.2016.070277.

[4] Al-AZZAM, Majed & Alazzam, Malik. (2019). Smart City and Smart-Health Framework, Challenges and Opportunities. International Journal of Advanced Computer Science and Applications. 10. 171-176. 10.14569/IJACSA.2019.0100223.

[5] Eckhoff, David & Wagner, Isabel. (2017). Privacy in the Smart City – Applications, Technologies, Challenges and Solutions. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2017.2748998.

[6] Sookhak, Mehdi & Yu, F. (2018). Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2018.2867288.

[7] Oliveira, T. A., Oliver, M., & Ramalhinho, H. (2020). Challenges for Connecting Citizens and Smart Cities: ICT, E-Governance and Blockchain. Sustainability, 12(7), 2926. MDPI AG. Retrieved from http://dx.doi.org/10.3390/su12072926

[8] Ismagilova, E., Hughes, L., Rana, N.P. et al. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Inf Syst Front (2020). https://doi.org/10.1007/s10796-020-10044-1

[9] Faria, R., Brito, L., Baras, K. & Silva, J. (2017). Smart mobility: a survey. In 2017 International Conference on Internet of Things for the Global Community (IoTGC). (pp. 1-8). Funchal: IEEE.

[10] B. Bowerman, J. Braverman, J. Taylor, H. Todosow, and U. Von Wimmersperg, "The vision of a smart city," in 2nd International Life Extension Technology Workshop, Paris, 2000, vol. 28

[11] T. Anagnostopoulos, D. Ferreira, A. Samodelkin, M. Ahmed, and V. Kostakos, "Cyclist-aware traffic lights through distributed smartphone sensing," Pervasive Mob. Comput., vol. 31, pp. 22–36, Sep. 2016.

[12] Mamra and A. Mamra, "A Proposed Framework to Investigate the User Acceptance of Personal Health Records in A Proposed Framework to Investigate the User Acceptance of Personal Health Records in Malaysia using UTAUT2 and PMT," Int. J. Adv. Comput. Sci. Appl., no. March. 2017.

[13] M. B. Alazzam, A. B. D. Samad, H. Basari, and A. Samad, "PILOT STUDY OF EHRS ACCEPTANCE IN JORDAN HOSPITALS BY UTAUT2," vol. 85, no. 3, 2016.

[14] M. B. Alazzam, A. Samad, H. Basari, and A. S. Sibghatullah, "Trust in stored data in EHRs acceptance of medical staff: using UTAUT2," vol. 11, no. 4, pp. 2737–2748, 2016

[15] V. Inukollu, S. Arsi, and S. Ravuri, "Security Issues Associated With Big Data in Cloud Computing," Int. J. Netw. Secur. Its Appl., vol. 6, no. 3, pp. 45–56, 2014.

[16] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, “Security and privacy in electronic health records: a systematic literature review.,” J. Biomed. Inform., vol. 46, no. 3, pp. 541–62, Jun. 2013

[17] Progress Vs Privacy - A Tale of Smart City Development in China. Memoori. (2020, December 8). https://memoori.com/progress-vs-privacy-a-tale-of-smart-city-development-in-china/.

[18] Tian, Ling & Wang, Hongyu & Zhou, Yimin & Peng, Chengzong. (2018). Video big data in smart city: Background construction and optimization for surveillance video processing. Future Generation Computer Systems. 86. 10.1016/j.future.2017.12.065.

[19] Kurnool, CS. (2016). Video Surveillance for Smart Cities. Cambium Network. https://cdn.cambiumnetworks.com/wp-content/uploads/2017/09/CS_Kurnool_04222016.pdf

[20] Haider Pasha, C. S. O. (2020). This is how we secure smart cities - what leaders must consider. World Economic Forum. https://www.weforum.org/agenda/2020/03/this-is-how-we-secure-smart-cities/.

[21] Jangirala S., Chakravaram V. (2021) Authenticated and Privacy Ensured Smart Governance Framework for Smart City Administration. In: Kumar A., Mozar S. (eds) ICCCE 2020. Lecture Notes in Electrical Engineering, vol 698. Springer, Singapore. https://doi.org/10.1007/978-981-15-7961-5_87

[22] Lim, Chiehyeon & Maglio, Paul. (2018). Data-Driven Understanding of Smart Service Systems Through Text Mining. Service Science. 10. 154-180. 10.1287/serv.2018.0208.

[23] Toma, C., Alexandru, A., Popa, M., & Zamfiroiu, A. (2019). IoT Solution for Smart Cities' Pollution Monitoring and the Security Challenges. Sensors (Basel, Switzerland), 19(15), 3401. https://doi.org/10.3390/s19153401

[24] Moser, S., Hahn, J. F., &amp; Fourie, P. (2017, July 23). Smart Cities and the Weather. Meeting of the Minds. https://meetingoftheminds.org/smart-cities-weather-22100.

[25] Zandbergen, D., & Uitermark, J. (2020). In search of the Smart Citizen: Republican and cybernetic citizenship in the smart city. Urban Studies, 57(8), 1733–1748. https://doi.org/10.1177/0042098019847410

[26] Fabi, Valentina & Spigliantini, Giorgia & Corgnati, Stefano. (2017). Insights on Smart Home Concept and Occupants’ Interaction with Building Controls. Energy Procedia. 111. 759-769. 10.1016/j.egypro.2017.03.238.

[27] La Vigne, Nancy & Lowry, Samantha & Markman, Joshua & Dwyer, Allison. (2011). Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention- A Summary.

[28] Gao, Yan & Schay, Alan & Hou, Daqing. (2018). Occupancy Detection in Smart Housing Using Both Aggregated and Appliance-Specific Power Consumption Data. 1296-1303. 10.1109/ICMLA.2018.00210.

[29] Jin, Ming & Jia, Ruoxi & Spanos, Costas. (2017). Virtual Occupancy Sensing: Using Smart Meters to Indicate Your Presence. IEEE Transactions on Mobile Computing. PP. 1-1. 10.1109/TMC.2017.2684806.

[30] Pratama, Azkario & Widyawan, Widyawan & Lazovik, Alexander & Aiello, Marco. (2018). Power-Based Device Recognition for Occupancy Detection. 10.1007/978-3-319-91764-1_14.

[31] Kleiminger, Wilhelm & Beckel, Christian & Santini, Silvia. (2015). Household occupancy monitoring using electricity meters. 975-986. 10.1145/2750858.2807538.

[32] Sorri, Andrea (2020, December 21). How does surveillance help make a smarter, safer city? Secure Insights. https://www.axis.com/blog/secure-insights/surveillance-smarter-safer-city/#:~:text=Smart%20cities%20use%20surveillance%20systems,people%20move%20in%20the%20city.

[33] Bartczak, Monika. (2013). The right to privacy in the legal system of the United States. Toruńskie Studia Międzynarodowe. 1. 5. 10.12775/TIS.2013.001.

[34] Solove, D. J. (2008). Understanding privacy. Harvard University Press.

[35] Aleisa, Noura & Renaud, Karen. (2017). Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions. 198-205. 10.5220/0006233701980205.

[36] Rouse, M. (2014). Internet of Things privacy (IoT privacy). http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-privacy-IoT-privacy.

[37] Lim, Chiehyeon & Kim, Kwang-Jae & Maglio, Paul. (2018). Smart cities with big data: Reference models, challenges, and considerations. Cities. 82. 10.1016/j.cities.2018.04.011.

[38] Abosaq, Nasser. (2019). Impact of Privacy Issues on Smart City Services in a Model Smart City. International Journal of Advanced Computer Science and Applications. 10. 10.14569/IJACSA.2019.0100224.

[39] Popescul, Daniela & Radu (Genete), Laura-Diana. (2016). Data Security in Smart Cities: Challenges and Solutions. Informatică Economică. 20. 29-39. 10.12948/issn14531305/20.1.2016.03.

[40] Cui, Lei & xie, gang & Qu, Youyang & Gao, Longxiang & yang, yunyun. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2853985.