A Proactive Systematic Approach to Enhance and Preserve Users' Tech Applications

Data Privacy Awareness and Control in Smart Cities

by

Edgard Musafiri Mimo

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved November 2022 by the
Graduate Supervisory Committee:

Troy McDaniel, Chair
Katina Michael
Kenneth Sullivan

ARIZONA STATE UNIVERSITY

December 2022

ABSTRACT

The reality of smart cities is here and now. The issues of data privacy in tech applications are apparent in smart cities. Privacy as an issue raised by many and addressed by few remains critical for smart cities' success. It is the common responsibility of smart cities, tech application makers, and users to embark on the journey to solutions. Privacy is an individual problem that smart cities need to provide a collective solution for. The research focuses on understanding users' data privacy preferences, what information they consider private, and what they need to protect.

The research identifies the data security loopholes, data privacy roadblocks, and common opportunities for change to implement a proactive privacy-driven tech solution necessary to address and resolve tech-induced data privacy concerns among citizens. This dissertation aims at addressing the issue of data privacy in tech applications based on known methodologies to address the concerns they allow. Through this research, a data privacy survey on tech applications was conducted, and the results reveal users' desires to become a part of the solution by becoming aware and taking control of their data privacy while using tech applications.

So, this dissertation gives an overview of the data privacy issues in tech, discusses available data privacy basis, elaborates on the different steps needed to create a robust remedy to data privacy concerns in enabling users' awareness and control, and proposes two privacy applications one as a data privacy awareness solution and the other as a representation of the privacy control framework to address data privacy concerns in smart cities.

DEDICATION

I dedicate this work:

To my lord and savior Jesus Christ, may this be a testimony of your unfailing love and strength towards your creature as your word in the Bible scriptures says in Philippians 4:13 – “I can do all things through Christ which strengthened me.”

To my wife, Sanctifiee Lushima Musafiri Mimo, may this be proof that love never fails as two are indeed better than one as your care and support for me and our children made it possible for me to focus and accomplish this goal.

To my lovely children, my daughter Sanctifiee Mimocrate Mwika Musafiri and my son Edifie Mimocrate Lushima Musafiri, may this be a reason to motivate you to follow your dreams and put yourselves to work to make them a reality. There is no limit to what is possible for you or your siblings to come, so may life give you the grace to find yourself a “Troy” that guides you, a “Katina” that encourages and challenges you, and a “Kenneth” that supports you along your way toward your goal and ambition.

To my father, Paul Musafiri Nalwango, may this be a reward for your investment and sacrifices that you devoted to me and more for the character of hard work and excellence that you engrained in me. Words cannot express the reality of your sacrifices made for me to enable grit and desire to pursue knowledge and enrich people’s lives.

To everyone like me who lost many loved ones and relationships along the way and who have had to be given up on for the cause of their destiny, may this be a symbol that you matter and that it is worth it for you to keep moving forward. Keep moving forward, only you were called for your assignment, so be bold and make it happen.

ACKNOWLEDGMENTS

I am forever grateful to God for the privilege, opportunity, and blessing to embark on and complete this doctoral journey with grace and favor towards me enabled by many miracles and miraculous connections to faculties, mentors, and peers.

Many thanks to my employer, Intel Corporation, for providing my tuition assistance support. I am especially thankful to the MPE/Sort organization within Intel via my manager Haritha for the encouragement and support in this journey. Likewise, I thank Arizona State University and the National Science Foundation for their funding support under Grant No. 1828010.

Words cannot express sufficient gratitude and thanks to Ph.D. committee members, namely committee chair Assistant Professor Troy McDaniel, Professor Katina Michael, and Professor Kenneth Sullivan for supporting me throughout my candidature.

Their supervision throughout has been better than I expected. Despite their demanding schedules, they have always given me quality time every time we met to discuss my research and open me up to more opportunities for both conference presentations and publications. You always encourage me and propel me to success. I also like to thank my fellow NRT colleagues and our NRT faculty mentors for leading by example in thoughts provoking research and drive to complete them.

I am privileged and blessed to have had throughout my educational journey several people that have helped me in different ways and seasons including my wife, children, parents, in-laws, siblings, friends, church family, mentors, and instructors. Thank you for investing in me and extending your love and help in many ways through encouragement and sacrifices that I may never be able to repay except through gratitude.

I particularly appreciate the constant support to thrive and excel of my beloved father Paul Musafiri Nalwango and father-in-law Alpha Lushima Shotshe, my regarded mentors Anthony Gould, Lemmy Meekisho, Hilda Asemsro, and my former coworker, research peer, big brother, and friend Jeremie Biringanine Ruvunangiza, and finally my Mimocracy and Mimocrates support crews. I want to thank my church families for their prayers and support as well as my pastor Anthony Gould for his constant encouragement in this journey. In different times and seasons, you have supported and encouraged me. My conscience condemns me to reference you briefly. Your numerous anonymous good deeds speak value to this journey and empowered me to press through when things and times got tough.

I am forever grateful to my lovely wife Sanctifiee Lushima Musafiri Mimo who has been my greatest motivation. She never allowed me an opportunity to lose sight of the goal – to use knowledge and solve problems that matter the most to make the world a better place. I could not have completed this study without her constant reminders to meet deadlines and her willingness to be the avenue for my knowledge dump as she was available to constantly discuss and question my ideas. Sanctifiee, your commitment to support and assist me in caring for our children throughout this time was vital, and it is because of God through you and our amazing children that I have completed substantial work in this journey.

You begin to learn the moment you realize that you do not know. All come empty, but no one returns empty

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

Figure Page

CHAPTER 1

OVERVIEW

Today, the question of privacy is very prevalent, especially when considering the digitization of personal data in tech spaces. Data privacy in tech applications presents a great opportunity to enhance the various approaches that have been proposed in research to enable privacy by design methodology. It is important to add to the principles of privacy by design methodology to accommodate an eighth principle that involves granting users control of their data and a larger say in what their data is used for even after they have provided it in tech applications. It is paramount to ensure that an individual's personal data does not get disconnected from them or used without their immediate consent.

The seven principles based on research of privacy by design necessitate that privacy efforts become proactive and not reactive as seems to be the current case [79]. Privacy in tech applications needs to be a default setting that users can tune and control to better own their personal information. There is a need to command that all tech applications be designed to embed privacy at all levels in the realization of the application's potential. The full functionality of the application technology needs to have privacy embedded from end to end to ensure data protection and security throughout the application's life cycle [79].

Privacy by design principles esteem that visibility and transparency are important for users as these principles are coupled with the principle that demands respect for user privacy. Thus, this research pointed at commanding and proposing the expansion of privacy by design principles to include users' data control as an eighth pillar to guarantee users continue to feel in charge and in control of their personal data.

It is necessary to add a user's personal data control principle whereby users are given total control of the personal data they provide in tech applications and get notified anytime their personal information is being used or sold for any purpose. To facilitate the user's data control, the design of tech applications must adopt a new paradigm of application development in connecting users to their data and providing a feedback mechanism for consent anytime personal data needs to be used or sold.

Making user data control another principle of privacy by design methodology will streamline an even more creative approach to a transformational technology that will help eliminate many unforeseen cyber-attacks as personal data will not be easily provided by users without the proper control of it. Users need to undertake a distributed responsibility to strengthen the development of better tech applications that serve their purposes without generating more problems. Creativity and persistence are needed to redefine tech application development to facilitate user data control in the current application development data control viewpoint.

The noble proposition of this dissertation is to allow advancement in technology to address the issues that various technologies have generated regarding the digitization of processes and systems in smart cities by focusing on better user personal data handling approaches. This requires identifying a way to incorporate the different technological innovations and address any potential issues and roadblocks to ultimately find a point or a sweet region of satisfaction where users feel safe and secure in the smart city while using tech applications and maintaining control of the personal data they provide in return. The question, therefore, arises in using tech applications as it pertains to users' data privacy is how users can regain control of their personal data and data privacy in tech applications. It is important to consider this question now rather than later to understand the gravity of the concern given the volume and scope of the different data and data types that are being collected by tech applications today [68]. The volume and complexity of data present a tremendous opportunity for embarking on the user data privacy journey. They ultimately guarantee users of their hands in not only providing data but in controlling what the data is purposed to do and how it is accomplishing that purpose. Technologies are lagging in enabling users to take control of their personal data after sharing it in tech applications because it might slow down the pace and numbers of tech application deployments as the user data-sharing workflow must be reimagined.

The incorporation of user data control in the tech space opens avenues for better data management control as privacy is concerned. Privacy is very relative in its aspect as it varies between different individuals and the importance of their personal information. Therefore, inviting users to help shape the tech application data management of their data is paramount to combat the various privacy violations that technologies have generated for decades. Understanding that most data or personal information about an individual does not drastically change over time. As a result, once the information is shared in tech applications, there is no appropriate way to preserve that information once it is tapped into.

Consequently, when someone gets hold of your personal information by chance through hacking or careless social engineering, it is almost impossible to overwrite or anonymize the information. Thus, it is important in securing the information and disposing of it when the users are not benefiting from it. In the context of smart cities, it is important to build and create a basis to define a skeletal disposition of what a typical application should be made up of in considering the various sources of data and the different data types available among the tech applications deployed in smart cities. This will encourage a deeper dive into assessing and categorizing what types of data citizens are sharing in tech applications and therefore associate the criticality of the personal data guardrails of protection and preservation.

Dissociating the data control that tech application owners have with that of users is a tremendous task that needs to be addressed sooner as there is already a larger volume of data that is collected and is being collected that does not contain user data control mechanisms. This is the biggest risk that is presented in trying to establish another way to represent and control data. The concept of user data control is a disruptive one for most tech applications today because most tech application owners may not entertain data sharing control in the sense that they can only control data that users provide to them with user-inherent restrictions. The scale at which data is collected and the pace at which data aggregation is done on the collected data to produce insights is growing exponentially to collectively constitute the Big Data ecosystem.

In smart cities, citizens are the major sources of critical data that reflect what activities citizens are involved in and what locations and things they tend to gravitate to. These insights perceived from the collected data enable smart cities to better allocate and manage their utility operating systems and resources in meeting the demand of citizens. In a more comprehensive sense, there is a certain level of tracking and surveillance that is necessary to efficiently predict citizens' demand and optimally manage the needed supply

[6]. Thus, it is paramount in considering the Big Data ecosystem of a smart city to realize that there is a need to properly collect citizens' data and strictly handle citizens' data in a way that citizens still maintain their data autonomy and full control of their personal data usage [26].

The smart city's Big Data ecosystem is reflective of the users that are contributing to it, and it is evident that there is a need to figure out how users can be allowed to control their data even after they have given it away, in the long run, to ensure that they remain safe and not easily disturbed in the digital space. The approach of user data control in the privacy-by-design methodology is novel because it reverts the data control process to the users themselves to determine what personal data tech applications can use and what tech applications can do in providing them with the proposed services. The user data control approach presents a remedy to the tech application privacy concerns by allowing the disturbances of tech applications to be controlled by users in facilitating users to proactively limit the number of tech applications they can be disturbed by. This is made possible by allowing users to simply not provide personal data or delete personal data linked to those tech applications.

The concept of privacy is defined as the right to be left alone, so in the context of tech applications, privacy can be elaborated as the right to only be disturbed by things or applications that one wants or allows to be disturbed by. In consideration of the privacy concept, it is crucial to ensure that users possess the key to unlock their disturbance in a sense by only interacting with tech applications they want to be disturbed by. In a more practical sense, it is paramount to consider how to manage the myriad ways of collecting data available in smart cities, implement data protocols and embed data control triggers with users' feedback at the point of data collection for all the different types of data collection that comprise the Big Data ecosystem in smart cities.

The Big Data ecosystem includes various kinds of data from atmospheric data to call record data to genomic data to e-commerce data to internet data to social media data to smart card data and internet data, and the list goes on and on [68]. Technology innovation in smart cities is not slowing up, instead, technology is rapidly evolving with newer types of data. Technology innovation generates many newer forms of cyber-attacks that jeopardize and compromise the Big Data ecosystem and users' personal data protection associated with it. Thus, it is apparent that the privacy of users' data needs strengthening, and users need to regain their personal data control back before data privacy risks grow out of proportion.

It is persistently judicious to get rather quickly to a point where user data privacy risks do not become overwhelming that the technological innovations coupled with the magnitude of data collection lock up the user data control avenues in proliferating more user data privacy risks. The proposed solution to begin to address and drive key ideas to implementation on how users can be given control of their personal data in tech applications start with the urgency of time to interrupt and intercept the deployed technologies and applications now sooner rather than later by employing the currently available technologies to enable the possibility of user data privacy control.

Knowing that citizens' data is important to enable smart city functions and operations, it is vital to focus on and assess the Big Data scope and its different aspects from data collection to data disposition passing through data processing and data storage. For example, when considering the aspect of data storage, it is no secret that smart cities possess a lot of archive information that is not even used, yet some of the archive information possess some relevant information about the users that can be used to profile them and violate their privacy especially when a malicious hacker breaks into the systems.

Thus, there is a necessity to reevaluate the usefulness of the archive data and at least dispose of the data that can be categorized as possessing personal related information enough to profile users bearing in mind citizens' migration from city to city.

Additionally, there are a ton of archive data that possesses information about people that have died which might be used in aggregation to help profile other individuals. It is another reason why smart cities need to have dynamic data and databases that can evolve with the data they possess to help reduce avenues of security issues and threats that can jeopardize the relevance of user data privacy control.

Smart city systems need to be actualized regarding most data that are generated in them, and they need to frequently be refreshed to take into consideration the evolution of citizens presently living in them. There is a great need to understand the data analysis that the collected information help fuel based on the produced outcomes to convincingly determine what essential amount of data needs to be collected, and in this way regulate the amount of data that users need to provide to receive the tech applications services.

As society continues to evolve, it is imperative to reevaluate systems relative to current citizens' behavior to transcend legacy system capability with current processes. It is important to focus on personally identifiable data about citizens or users because most of this data does not change over time [54].

So, if it is hacked once, then that information will be in the hands of another individual, and the victim may not be in control of their data. As result, the individual cannot be afforded the privilege to determine when they can be disturbed and by what. For example, information about someone’s birth date does not change over time, and information about someone’s health history or past physical addresses does not change over time, so it is paramount that this information is well secured, preserved, and more importantly collected only in certain classified and restricted tech applications for specific reasons that users deem more valuable.

When someone else gets control of citizens’ personally identifiable information that does not change over time, they do not have to struggle much to reobtain the data, and this leads to citizens not being the only ones who can control their data. Thus, there is a need to transition from a static state of data to a dynamic state of data where the personal data possesses not only the content but also the user approval direction to determine whether it should be used, kept, or discarded.

This is relevant as users’ interests change over time as they evolve by gaining new insight and new knowledge, so the relevance of their data also changes together with the application’s proposed values. It is therefore a great avenue and opportunity to begin to assess tech applications data, categorize the data and dissect the data to better understand how the collected data relates to users, and how they can keep control of the data even though the data is shared in tech applications [26]. In the effort to categorize the data, it is crucial to make sure that there is definite attribution of each data and data type association to a dedicated category whether personal or impersonal [26].

All the data that is collected in the smart city can be classified into mainly two different categories namely the personal category and the impersonal category [54]. Personal information is associated with any information that can characterize an individual, so any personally identifiable information in any of its forms whether it is in structured form or unstructured form [26]. If the collected data can characterize an individual among many, this piece of data is deemed critical and of great concern in data privacy research and scope because it possesses an avenue that can be exploited in violating the individual's privacy.

Another point of concern is the different kinds of data types that are readily available in the smart technology space that enable the collection of data in tech applications. As technology is evolving, more data aggregation and data type combinations are taking place. Consequently, it is paramount to determine schemes that will facilitate dynamically attaching or attributing user data control to the data content and data types to ensure that users remain the deciders of what their personal data is used for. The data collection process needs to be redefined by identifying the source of the data types and the owner of the data and creating an unaltered relation between the data, its provisions, and its owner.

For structured data, it is noticeable that the allocations of private information they contain can be detected by currently available systems and methods to quickly gain ground in enabling user data privacy control in tech applications. As for unstructured data, it is more convoluted as the content and the data type combinations present a bigger data privacy detection complexity for many false positive and negative alarms, besides it requires more and more computing power in the data assessment process. If a picture is worth a thousand words, what can one say about a recorded audio, and what can be said about a recorded video?

All the unstructured data types reflect in more detail the dynamics that characterize users to the point where research has shown that an aspect of a smart city can be characterized just based on some data showing the affinities and the interests of people living in that smart city [6]. Thus, in the context of privacy, most privacy issues are very personal, but in the context of smart cities, smart cities need to provide a collective solution to their citizen's data privacy issues. From a user's personal level of data privacy issues and concerns, there is a need for a collective solution that needs to address and remedy the effect of personal privacy implications. If smart cities must succeed in the resolution of users' data privacy, it is crucial to embark on the design of the user data control approach so that the modern data analysis can be adapted to the approach and tuned to facilitate the future deployment of algorithms that support the user data privacy control progress in tech innovations.

Most algorithms and AI innovations are enabled and effective due to the abundance of data that help to even minimize and flag inherent biasing, which otherwise would not have been possible. Data generated from algorithms and models because of user personal data should also be treated with much care to ensure that is not connected to the users it originated from, otherwise, the users must possess some level of control over the generated data as well. The encouraging fact in today's innovations is there is a lot of progress and emphasis on data protection although it is not enough.

The simple investment in more robust data protection efforts and mechanisms speaks value in the acknowledgment that most smart city systems are essential and must remain operational. Nevertheless, these systems are not flawless meaning if they are not protected, they are susceptible to failure. When data protection design and method are not perfect, there are even greater data privacy risks that affect users, which many users are not aware of. As users get more informed on how the use of their digital data is affecting their privacy, users will begin to boycott the adoption of tech applications unless they are completely convinced that they are in charge and in control of how their data is being used.

The issue of user data privacy is serious in tech applications because most tech applications' owners are mostly focusing on combating the data security issues that affect their users' data without placing an even bigger emphasis on the data privacy risks associated with the abundant volume of data collection. As more data is collected, generated, and controlled by just the application owners and their associates, users will demand sooner or later the control of their data should more and more privacy risks and threats begin to surface.

If data is not robustly protected, and user data privacy risks begin to surface, users will wrestle among themselves to determine whether the tech applications are more beneficial and valuable to them than their personal data. The advantage of tech applications' services and the loss of data control will present an inflection point for users to decide what is best for them. The big decision users must make is to decide whether to trade their personal information in return for the tech applications' services they are getting and at this point, it might be detrimental to both tech applications' owners and users.

Tech application data disposition is also very critical in eliminating the data privacy risks that users can incur. It is fundamental to understand how data is deleted in tech applications and the frequency of data disposition to reliably allocate proper disposition frequencies to more sensitive personal data. As mentioned earlier, there are a lot of archived data in smart cities that serve no real value as they are no longer used, yet they possess the potential to be easily hacked and jeopardize the privacy of many users in the process. The frequency of personal data disposal and the mechanism of personal data disposal need to be reassessed to proactively prevent many avenues where data privacy flaws can be maximized.

To allow users to be in control of their data, it is important to focus primarily on what digital privacy means for users without intermingling the issue of privacy together with the issues of data security although they are interdependent. The proposition of this dissertation mainly focuses on data privacy and addresses the different facets of data privacy from the point of data collection to that of data disposal through the lenses of users. It also discusses the current digital tech possibilities needed to enable user data privacy control in tech applications. The proposition assesses the how, why, what, when, and where data is collected and shared in tech applications to the point of data deletion and storage.

In the context of smart cities and the 3D citizen value-motivated privacy basis, it is essential to understand and quantify the actual value that the tech applications present to users that justify the investment to command the collection of personal data. The value of the different tech systems or applications in smart cities is determined mainly by the data that enables the operation of these systems and the objectives of these systems in the first place, which justify the reasons for their creation [54].

The 3D citizen value-motivated privacy basis presents the proper basis to assess tech applications as they relate to users and their personal data in considering three different dimensions axes namely the data axis, the purpose axis, and the value axis respectively. The axis of data deals with what kind of data is used to enable the tech application that is being assessed [54]. It is very important to understand for each tech application what kind of data is enabling it to operate and function to provide its intended services. The next preoccupation of the data axis resides in knowing what type of data is used in enabling the tech application's operation and function. Is the tech application enabled by personal data or impersonal data?

Impersonal data includes data like weather forecast data or air quality data since no one can rely on them to identify or profile a specific individual. Based on the data dimensional axis, any tech application using personal data needs to be assessed, addressed, and redesigned to include the user's personal data control mechanism. Another preoccupation with the data dimension axis resides in knowing why the data is needed, collected, and used in the first place.

This preoccupation leads to the curiosity of understanding what is the purpose of using personal data in enabling the tech application. This is where the second-dimensional axis of purpose finds its roots by defining where the tech application aims to provide a service to the users or by providing a mean of user surveillance by the tech application owners or stakeholders. It is fundamentally crucial in smart cities space to assess all the tech applications and categorize them based on their purposes and actual functions and operations to identify whether they enable services to users or surveillance of users [6]. Many deployed tech applications today that use users' personal data are acting as tracking devices as they track people's movement and affinity using their people’s requests data and predicting what decisions people can make next. Some tech applications collect user personal data even though most of the users’ personal data does not play any role in enabling the application’s functionalities. In this case, it is important to understand how the tech applications benefit by using users’ personal data that is not required to enable their functionalities in any way.

The remaining dimensional axis of the 3D citizen value-motivated privacy basis is the value axis where each tech application is assessed in determining what proposed value it is offering to users to justify the collection of users’ personal data. In the context of smart cities, the value dimensional axis is indispensable as it helps determine whether a particular application technology is an answer to the city’s problem, the citizens' problem, or both.

Understanding the value of the proposed solution of each tech application is key to unlocking the realization of privacy-preserving tech applications because tech application makers will be pushed and forced to understand, validate, and defend why they need users’ personal data. It is apparent considering the value dimensional axis that there are tech applications in smart cities today that are more valuable for the cities than the citizens, and yet collect most of the citizens’ personal data to facilitate their surveillance. These are mainly tech applications that are not created for citizens’ added value, but for the city to make the city operates better by knowing the different choices and preferences of its citizens. This is done through a systematic analysis of users’ inputs that are leveraged to channel the city’s decisions in a certain direction to better realize the citizens’ needs. Nevertheless, there are likewise some tech applications in smart cities that are more valuable for citizens than cities, and as such maybe provide more value to citizens than to cities.

Hence, the concern of data ownership and control becomes critical to the long-term survival of tech applications and systems that predominantly rely on user personal data. Citizens that are providing personal data to feed many smart cities' tech applications and systems will soon demand to have control of their personal data and their data privacy regardless of how they primarily shared the information once data privacy risks and issues begin to surface.

It is crucial in smart cities to understand the types of personal data used and who controls that data. It is also stimulating to know how data management is performed in the instance of user migration or citizen migration from one city to the next. The question will be whether the city discards the data of the individuals that have migrated to another city or do the cities still retain their data and if so, for what reasons.

The 3D citizen value-motivated privacy basis facilitates the assessment of tech applications in creating operational spaces for tech applications and systems which are associated with different privacy levels based on the tech applications' functionalities, the data requirements, and the user privacy feedback and concerns. The intersection of the three framework dimensional axes creates eight different tech operational spaces where data privacy can be considered and measured for a particular technology or application given its provided service.

The first operational space is a tech operational space where technologies or applications that use citizens' data to provide citizens value for surveillance purposes are found. It is critical to understand for example citizens' concerns about the deployment of cameras everywhere for security reasons. Is it appropriate to deploy these cameras for citizens, or do they control the video data collected through cameras? As these questions are considered with the advancement of technology empowering face recognition, individuals can easily be profiled.

Thus, the question of curiosity regarding data control arises to understand under what circumstances the captured videos get deleted or if there are no major incidents captured in the collected videos for a long period. The key aspect of the framework is in understanding tech applications and classifying them in the different operational spaces to better assess and regulate how much user personal data the tech applications must collect to fulfill their proposed value [54].

It is important to appreciate that personal data have different data sensitivity levels that need to be well-thought-out in the data handling process [26]. Some personal data in tech applications are being collected without the users' awareness and conscious data-sharing permission. The reality with tech application users is that most of the users do not take tech application consenting seriously, and almost none or very few among them dedicate their time to reading the tech applications' terms of service or updated terms and conditions for web or mobile applications.

When users' sensitive personal information is shared by tech applications that the users consented to without fully understanding the applicable terms of service, users' privacy may be violated although there was unintentional consent. Many tech application users in smart cities are willing to share non-sensitive personal information with no major explanation required, but they require some rationale for sharing sensitive data.

In the context of user data privacy, the framework enables an easier way to focus on tech applications that fall in the operational spaces that use personal data. It helps drive more research work and interest in investing time and resources in tech application development to facilitate the transition of tech applications from using personal data to using impersonal data while still providing the same value to users. There are two different apparent states of tech applications namely a state where value is provided to users based on the personal information users share in the tech application and a state where value is provided to users based on information considered impersonal.

Thus, it is paramount in the preservation of user data privacy to invest in the redesign of tech applications that use personal data to tech applications that will use impersonal data while providing the same value to users. It is only by understanding the value of tech applications that users are willing to trade their personal information for that the smart cities will be able to fundamentally define the threshing line between what information users consider as sensitive and what they consider non-sensitive.

The privacy-by-design principle of transparency will benefit greatly from the tech applications' user-proposed value to facilitate the possibility of tech applications providing value to users without personal data. If more tech applications in smart cities gravitate toward the enablement of providing user value without using personal information, then smart cities can begin to become more resilient toward data privacy risks. Smart mobility tech applications in smart cities ultimately use personal data to provide service value for the city efficiently and optimally to help manage traffic jams, required numbers of transportation based on demands, the number of people commuting around the city, and so on.

The first operational space of the framework is associated with a high privacy level rating because the value given to the city by the tech applications in this operational space remains heavily dependent on users' personal data which offers direct and indirect tracking opportunities through users' requests query and location [54]. Most smart mobility systems and applications in smart cities today use predictive algorithms based on past users' data to better optimize the duration and nature of a commute based on users' demands and logistics. It is crucial to be mindful of the element of users' migration that must be filtered in or removed to eliminate some user data privacy risks for migrated individuals.

The next operational space of the framework is associated with a high privacy level rating together with a more citizen-focused value where systems and tech applications in smart health operate. It is extremely challenging and almost impossible to provide a specific type of health treatment or requirement to citizens for their well-being without knowing basic information about their health history. Thus, tech applications in this operational space must capture users' personal data to classify individuals into different categories based on their needs so that the tech applications' services can match the users' demands. In smart health applications, the remedies are based on and are proportional to the related provided personal information based on the individual symptoms, allergies and previous surgeries, and health history depending on the tech applications. Thus, using personal data to provide some services to citizens is necessary for smart health tech applications, but still collecting a lot more personal data than needed presents greater privacy risks especially when users do not hold a share in controlling their provided personal data.

Some tech applications in smart cities are associated and flagged with the highest level of privacy risks rating because of the surveillance component that the tech applications enabled for the cities without a user's data control effect. Some tech applications in this bracket involve many smart e-government and e-governance applications where users are required to be authenticated and verified to be able to participate in activities like voting. It is important in this case to ensure that the voter is a citizen of the city and discard any outsider votes that can jeopardize the outcome of the voting event. Most tech application authentication processes in these applications require multiple factors to authenticate users to the extent of requiring government IDs to validate those users are whom they claim.

Most smart e-government and smart e-governance applications require users to provide additional pieces of evidence in conjunction with their government's IDs like a utility bill or a personal letter. The smart e-government and smart e-governance applications fall into the remaining two operational spaces that are associated with user personal data and the surveillance objectives of tech applications. This is where user data privacy control can play a major role to drive the redesigning of tech applications to incorporate user data privacy control as an additional principle to the privacy-by-design methodology.

There are different operational spaces associated with tech applications that provide value and services to citizens without using sensitive personal data such as smart home tech applications where all the home operations and utilities are operated efficiently to meet the demand of the users.

The 3D citizen value-motivated privacy basis presents likewise the idea of impersonal data surveillance of citizens and the possibility of citizens gaining value from tech applications that do not necessarily require user personal data to function [54]. These tech applications include open data applications and some parental guidance applications. It is important to consider the fact that children of today's smart cities are the main citizens of tomorrow's smart cities, so it is important to ensure that parental guidance applications do not facilitate children's surveillance to the point of profiling them [54].

It is critical to ensure that the parental consent applications are not used by the city or the application stakeholders to control the future of children in smart cities by influencing their education and integration. It is decisive to identify tech applications that target children, consider the services they enabled for them, and assess whether they track children's queries and locations to safeguard long-term data privacy resilience.

The reality of smart city tech applications' user data privacy risks today is not far-fetched. It is more apparent nowadays as more cyber-attacks and security breaches are affecting tech applications and compromising the digital data ecosystem in smart cities. Highlighted letdowns and flaws in the security-by-design approach showcase to a larger degree some lack of awareness of the evolutions of different kinds of data security threats ranging from social engineering to software misses and bad practices. The amount and frequency of software patches to respond to security glitches highlight the extent of the reality that digital data management is facing.

Some solutions have been proposed to remediate some parts of the problem, but these solutions are not sufficient. The approaches that smart cities have taken in large part are to strengthen and invest in data security mechanisms, with few of these solutions attempting to address the data privacy concerns to some extent.

Some of the proposed solutions include the data anonymization technique which is an approach where the collected personally identifiable data is processed to strip out any connections with the individual it originated from. This method has been proven to work in some cases, nevertheless, some de-anonymization techniques recently demonstrated that through data aggregation users can still be profiled from the anonymized data [80]. Thus, the anonymization technique can be considered a loose solution for the time being as robust solutions are being developed. Another apparent solution is the pseudonyms technique where personally identifiable data is collected from individuals and attributed fictitious characteristics to it. Data aggregation has also proven that pseudonymized data can still be used in identifying and profiling users [80].

Another prevalent solution is blockchain due to its attributes of proving its robustness in terms of data security and transparency generated from unaltered nodes whose data remains immutable. The privacy concern in the blockchain is the fact that data is shared with everyone in the network for transparency's sake, yet some of the data may contain personally identifiable information that is accessible to others in the network. The fact that everyone has a record of all the transactions in the network presents an opportunity to apply blockchain in the user data privacy control approach to consolidate and control the user's personal information.

It is important to capitalize on blockchain technology to help facilitate user data sharing blockchain networks where users possess different blockchains of their data to track and understand how their data is used by tech applications. It is a novel approach to help users have their own set of blockchains where each application that uses personal data gets consent from the user and enables the user data control mechanism.

Another solution in smart cities is using encryption mechanisms to enable data security and control so that users provide their personal data to tech applications with encryption tokens containing an expiration duration that invalidates the shared personal data when expired. This kind of encryption mechanism will facilitate the deletion of personal data so that it does not remain stored in tech applications when not in use or beyond the user's permitted duration. This approach commands an active interaction with users who provide their personal data to always consent or decide not to share their personal data anytime.

It will minimize the number of users signing up for tech applications and consenting to web applications unless they have some value to gain from the enabled tech applications' services. Many users signing up for mobile applications and consenting on websites do not even remember when they consented and the data they shared. Some critical problems must be resolved to better solve tech application data privacy issues. The main issue is about the software service agreement or terms of use of applications that are generally ignored by users.

Most software services agreements are not very clear with the relevant details that users must quickly know because they are generally long, and most users do not read them. Most users are so desperate to start using tech applications and enjoying what tech applications provide to them, so they end up agreeing to the terms of use without reading them. Thus, it is paramount to facilitate the assimilation of these terms of use clearly and straightforwardly for users to quickly decide whether the proposed tech application value is beneficial to them to justify their sharing of personal data.

The software service agreement or terms of use deals with two main issues that are critical in the context of data privacy namely the issue of data management and data ownership. It seems rather tricky that tech application companies use words like third parties or associates whom they share the data they collect with without listing these stakeholders for users are aware of the extent to which their data is going to be shared. Thus, users must know where their data is being shared and what to expect from their data if it is being misused, so the data privacy blockchain approach to enable data privacy control is key because it will enable users to have the ability to know how their data nodes are being connected and get the information of who has access to it.

It will allow users to know which organization is using their personal data such as name, and smart card information, and contact them to find out for what purposes. This approach will help raise users' data awareness which is crucial to solving most of the data privacy issues in tech applications.

It is important to consider the duration and usability of data to minimize the need to archive data and command tech applications to hard delete personal data more frequently especially when not in use. Most users that share their personal data do not even care about the deletion frequency and deletion methods use. One aspect of data privacy that needs to be addressed is data management with software services as well as data protection with encryption mechanisms to help streamline the data collection process at every point of data collection.

It is important because devices that are used for data transfer from one system to the next also face security issues that can compromise data. It is important to understand data privacy risks associated with data transmission from its point of collection by an IoT device to the cloud while passing through several network layers and in different data packet portions. The complexity requires to secure data transfer increases, even more, when security protocols are added to combat network interruptions that occur in packet division and shift to ensure that data reaches its end point uncompromised.

The information communication and technology known as the ICT network possesses systems with security issues due to different devices having different data security protection levels. Thus, the most pressing question considering the future of tech applications in smart cities is how citizens can regain control of their data and data privacy.

The objective is to address the issue of data privacy as an independent issue in smart cities and disconnect it from all the interdependent issues that are associated with privacy such as security, cost, discrimination, surveillance, time, and control to name a few. All these issues are associated with privacy somehow, but when the definition of privacy as the right to be let alone or to not be disturbed is concerned, it becomes apparent that the issue can be addressed independently when considering the standpoint of users regarding the value of their data.

This dissertation starts with an overview of the smart city space by discussing the technologies that enable smart cities in generating what constitutes the Big Data ecosystem that is used in enabling data-driven decisions. Data and data sources are then explored with a focus on data security issues that create data-induced privacy issues. In exploring data privacy issues, the dissertation focuses on personal data handling and collection in smart cities as well as discusses why citizens share their personal data in the first place.

To understand the relationship of personal data in the smart cities space with the purpose of tech applications and how citizens view it, this work discusses the 3D privacy basis to help discover a dimension that enables solutions to data privacy issues in tech applications. The 3D privacy basis identifies a critical dimension that simplifies how to handle personal data from the citizens' perspectives. Based on the 3D framework, a proposal to encourage private information characterization and classification methods for different data security levels based on the value of the information is made.

The dissertation then elucidated the importance of the 3D framework by running a tech data privacy survey that validated that indeed users view some personal data as more important than others. And as such, there is a need for more data privacy awareness and control for users to aid in addressing data privacy issues in smart cities. This dissertation concludes with the proposition of two prototypes of privacy applications namely the privacy awareness mobile application and the privacy control web application to demonstrate the feasibility and possibility of empowering users to be aware and in control of their data while using tech applications. Figure 1 below shows the dissertation's objectives and milestones as they relate to the different chapters.

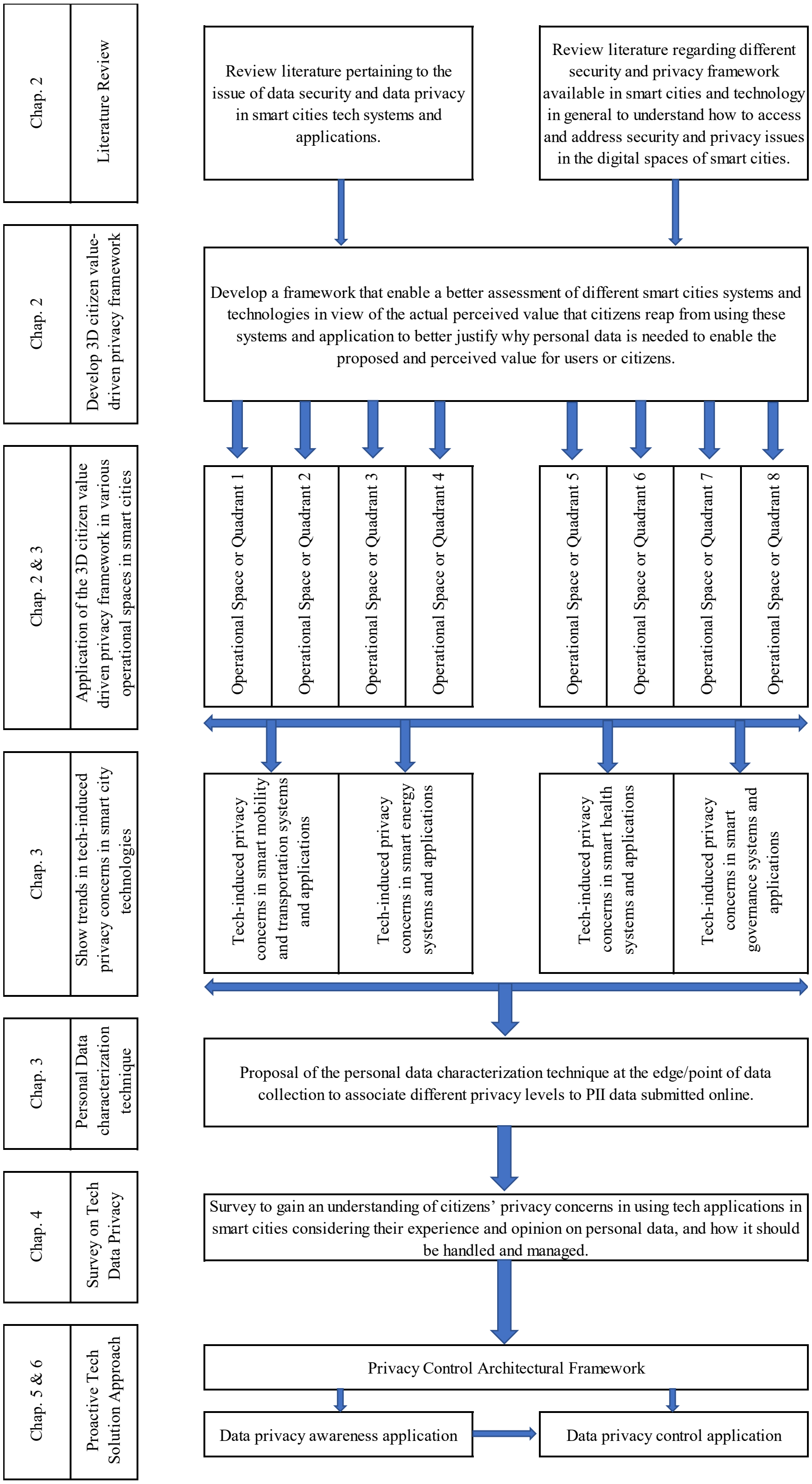

Chap. 2
Literature Review
Review literature pertaining to the issue of data security and data privacy in smart cities tech systems and applications.
Review literature regarding different security and privacy framework available in smart cities and technology in general to understand how to access and address security and privacy issues in the digital spaces of smart cities.
Chap. 2
Develop 3D citizen value-driven privacy framework
Develop a framework that enable a better assessment of different smart cities systems and technologies in view of the actual perceived value that citizens reap from using these systems and application to better justify why personal data is needed to enable the proposed and perceived value for users or citizens.
Chap. 2 & 3
Application of the 3D citizen value driven privacy framework in various operational spaces in smart cities
Operational Space or Quadrant 1
Operational Space or Quadrant 2
Operational Space or Quadrant 3
Operational Space or Quadrant 4
Operational Space or Quadrant 5
Operational Space or Quadrant 6
Operational Space or Quadrant 7
Operational Space or Quadrant 8
Chap. 3
Show trends in tech-induced privacy concerns in smart city technologies
Tech-induced privacy concerns in smart mobility and transportation systems and applications
Tech-induced privacy concerns in smart energy systems and applications
Tech-induced privacy concerns in smart health systems and applications
Tech-induced privacy concerns in smart governance systems and applications
Chap. 3
Personal Data characterization technique
Proposal of the personal data characterization technique at the edge/point of data collection to associate different privacy levels to PII data submitted online.
Chap. 4
Survey on Tech Data Privacy
Survey to gain an understanding of citizens' privacy concerns in using tech applications in smart cities considering their experience and opinion on personal data, and how it should be handled and managed.
Chap. 5 & 6
Proactive Tech Solution Approach
Privacy Control Architectural Framework
Data privacy awareness application
Data privacy control application

Figure 1: Dissertation Objectives and Milestones Related to Chapters

CHAPTER 2

PRIVACY AND SMART CITIES

2.1. Literature Review

Privacy is a vital component that smart cities must carefully address to win citizens' adoption of their initiatives. It is the most important component when enabling citizen-centered smart cities. Privacy as a notion delineated fundamentally as the individual's right to be let alone [1] has expanded over time. Privacy comprises several aspects, for example, freedom of thought autonomy, the right to self-isolation, and the capacity to own and control personal data and information. It also involves freedom from surveillance of any kind, the defense of one's reputation, and protection from investigations and searches even in the digital space [2].

The vision of privacy in the context of data privacy cannot be weakened with the widespread development and deployment of IoT sensors in smart cities space that progressively amass personal information from both private and public sectors and institutions [3]. Data privacy concerns are accentuated due to the massive collection of personal data in various shapes and forms sometimes with or without people's granted consent and awareness [4].

Almost all useful smart city technologies that enable most innovations and value-added services to citizens whether it is machine learning, cryptography, biometric analysis, blockchain, artificial intelligence, 5G, and so on, require massive data collection. The data collection incorporates to a bigger extent the collection of personal data that induces associated privacy concerns that need to be appropriately addressed to elude a technological data privacy invasion of citizens or users.

Accordingly, technology-driven data privacy issues among citizens within smart cities occur in many different forms pertaining to the volume of data collection and its content. There is a necessary shift to consider moving from quantifiable data collection through IoT sensors to automated computational data modeling analysis that empowers services for citizens. Data privacy concerns in the digital space are vast and multifaceted to dichotomize and resolve especially with the collection of more and more data without appropriate regulations and protections in place.

Privacy in the digital space remains the prerequisite constituent in producing an effective and defensible technological value for citizens [5]. Every technology that collects, interacts, or aggregates citizens' personal data must provide its value without aggravating data privacy concerns among citizens. Technology-motivated data privacy issues transpire and evolve throughout the tech lifecycle. Tech-driven data privacy issues are inevitable from the tech idea conception to development to deployment and more importantly during the lifetime of the technology, its applications, and use.

For technologies that deal with personal data, there is an ever-present risk of data privacy that must be flagged throughout the lifespan of the technologies because of their affiliation with people's personal data that requires users' long-term awareness, consent, and willingness to grant the technologies permission [6] to handle and interact with their information. From the tech application conception phase, data privacy must be addressed so that appropriate data handling mechanisms can be put in place.

In the tech application development phase, privacy concerns [7] are inevitable [8] considering how personal data should be used and protected to guarantee no unauthorized third party can access it. This is required to avoid potential data compromise and unauthorized access to people’s personal information without their conscious agreement and authorization.

In the tech application deployment phase, likewise, data privacy-related issues occur as data security and data aggregation transpire for various purposes including malicious ones as hackers may exploit more than intended information from data available to them for other uses without authorization [8]. Finally, in the tech application utilization phase, data privacy concerns arise even more from different viewpoints sometimes from the accumulation of data, other times from different database security protocols and systems [9], all of which interact with data in various forms.

The datafication of smart cities requires a prompt and proactive data privacy defense approach to avoid generating more avenues of privacy breaches with unnecessary data collection. Smart cities’ information and communication technology empower tech infrastructures capable of facilitating extensive personal data monitoring. ICT can facilitate as well, without inducing privacy concerns, proper management of city utility and maintenance systems, proper mobility means, appropriate air and water quality monitoring, efficient energy utilization, effective neighborhood sentiment consideration, etc.

The digitization of smart city technologies excavates paths for data privacy and security apprehensions that demand in-depth evaluation and preservation of the expected citizens’ tech value without data privacy compromission [26]. The Big Data [10] generated by interactive multimedia platforms and services consist largely of unorganized data, and these platforms and their contents are frequently the targets of cyberattacks [11][13]. The systems and methods gathering and creating multimedia massive data [12] and the acquired data itself are vulnerable to cyberspace security risks since any fault in the intelligent multimedia ecosystem may instantly compromise the systems and users' data. There is no underestimating the opportunity presented by security concerns in visual systems for smart cities to facilitate progress in face recognition [14][15] and mood [16] detection [17] and identification systems.

Visual systems provide several privacy risks that cannot be ignored, particularly as they continue to provoke public apprehension. Concerns about the data security risks that attack tech platforms and technologies have yet to be completely utilized for the advantage of smart cities, and that applies to audio synthesis systems. When it pertains to intelligent multimedia platforms and technologies, there is a wide variety of risks [13][17] that ought to be evaluated to guarantee the protection of individuals' personal information in smart urban environments.

Risks to data privacy and security of adaptive multimedia systems can arise at any stage, from the time data is captured by a camera or any recording device to when it is processed [17] or stored [10][13][18] in data centers. Consequently, it is important to think about the broader privacy ramifications for residents of smart cities, especially if the data captured includes details about several people living in the same smart city who may have distinct privacy needs.

The digital multimedia monitoring ecosystem [12] depends on a wide variety of technological breakthroughs, but the inclusion of sound and video devices and technologies remains a fundamental pillar of the digital multimedia infrastructure. Multimedia data sources consist of audio, pictures, video, sensory signals, and linguistic data that include crucial information concerning the environment and nearly anything in it, including humans.

Over the past decade, advancements in machine learning and artificial intelligence have allowed for a more accurate interpretation of social environments, which in turn has led to improved decision-making [10][19]. It is easy to gather comprehensive auditory and visual details about residents [6], such as their voices, faces, and movements [20], which may be utilized in characterizing and distinguishing an individual. This is made possible thanks to the widespread deployment of sophisticated multimedia technologies in smart cities that complement and augment conventional surveillance techniques through a decentralized architecture that supports multiple types of sensors and cameras [26].

2.2. Smart Cities and Technologies

The importance of smart city planning with residents' safety and happiness in mind is laid forth, along with some of the benefits and drawbacks of the above technology elaborated. Some data privacy and data loss prevention technology, such as blockchain technology, cryptography, anonymizations, and federated learning, are discussed in this chapter. The purpose of the discussion is to demonstrate the various control and accountability measures that can be implemented to create a smart city that is environmentally friendly, self-sufficient, and data privacy-preserving in the long run.

There is a great number of technologies that are essential to allow and enhance smart city efforts, namely the 5G network, Internet of Things, Artificial Intelligence, Information and Communications Technology, Big Data, Blockchain, Renewable Energies, etc. These technologies as shown in figure 2 below are explored to provide a clearer understanding of what comprises the many flavors of smart cities efforts.

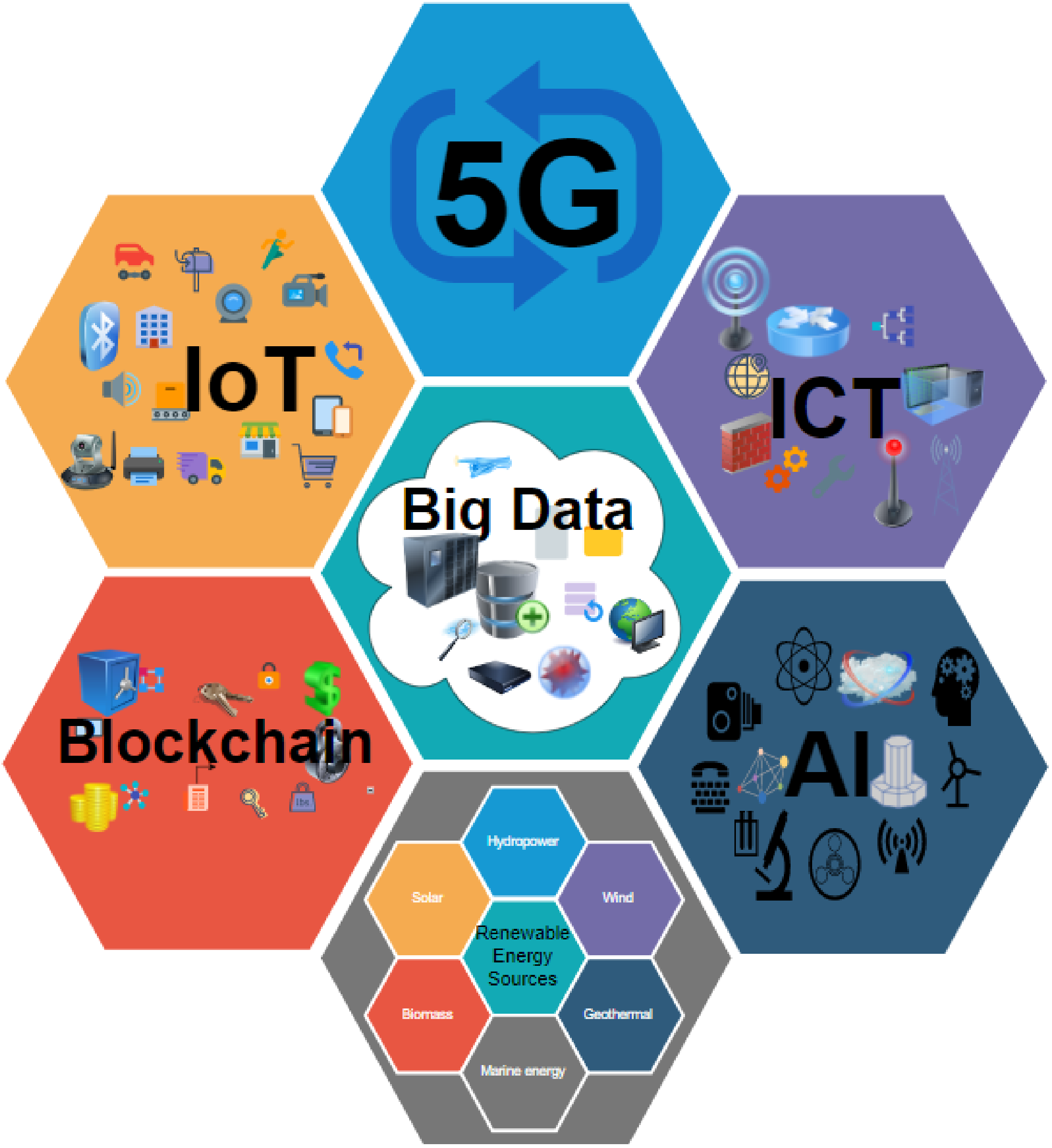


Figure 2: Foundational Technologies Enabling Ubiquitous Smart Cities.

2.2.1. 5G

5G, or the fifth-generation wireless communications mobile network, provides significant enhancements over its predecessors, as well as new avenues for connectivity and communication that fuel plenty of technological innovations and inventions occurring today and in the foreseeable future [21]. The world is now experiencing a digital transition, and 5G is a fundamental constituent of this transformation. 5G provides significant improvements over all the mobile generation wireless networks that came before it. It is the reason that makes most of the smart city initiatives viable today. Extreme mobile broadband, enormous device communication, and ultra-reliable limitless information exchange are the three types of consumer incentives that 5G technology enables [22].

Extreme mobile broadband makes it possible to have high-speed internet access with greater bandwidth and tolerable latency. It also offers the capacity of streaming films in UltraHD and brings the prospect of media that uses virtual and augmented reality to life, in addition to providing several other advantages. Furthermore, the huge machine-to-machine communication powerfully enabled by 5G makes it possible to enable long-range and broadband machine-to-machine communication at a price that is theoretically somewhat cost-effective, while at the same time it enables the reduction of the amount of power required and used in the process.

5G opens the possibility of offering a service with a fast data rate and low power consumption, all while having expanded coverage thanks to a decreased amount of controller performance that is spread over many cell carriers and designed for use in IoT applications [22]. 5G possesses a limited, super-duper connection that has the same potential to provide a connectivity service with a high quality of service that is impossible to achieve with the standard mobile network generation design.

Its primary purpose is to provide real-time communication, which in turn makes it possible to implement cutting-edge technologies such as intelligent grids, automotive communication, smart transport systems, industry 4.0, telemedicine, and many others. It is important to emphasize that 5G is far quicker than 4G and that it allows more remote-controlled processes to be carried out via a network that is extremely dependable and has the potential to have zero latency [22].

The 5G spectrum may be roughly split into two halves namely the “millimeter wave 5G" and the "6 GHz 5G". The millimeter wave 5G is an integral technology of the 5G network that allows high-performance network connection. In contrast, the 6 GHz 5G function as a mid-frequency band that works halfway between coverage and capacity to offer a smooth environment for 5G connectivity [22]. This difference is what distinguishes the millimeter wave 5G from the 6 GHz 5G. The 5G spectrum at 6 GHz is intended to provide a high bandwidth while also improving the performance of the network [22].

When the mid-band bandwidth is not available, the 6 GHz 5G connection offers continuous channels that assist to reduce the need for network compression. This not only makes the 5G connection accessible to users wherever and at any time, but it also makes it more inexpensive for them. On the other hand, the millimeter wave 5G offers a variety of connection services, which encourage practically all network beneficiaries to include this technology as part of their 5G deployment planning and aspirations.

The millimeter wave 5G is already being deployed by several service providers, and data from their simulations reveal that the millimeter wave 5G bandwidth has the potential to be utilized much more than it is already being used owing to the potential that it already contains. The millimeter wave 5G bandwidth enables the next generation of mobile networks by providing reliable wireless communication in addition to an extremely large bandwidth [22].

The 5G wireless communications mobile network is more than just an evolutionary advance over the previous generation of wireless network technology. It is a technology that has the potential to change the world since it has the goal of removing the network limitations that now exist in terms of access, performance, capacity, and latency constraints on global communication [23].

5G has the potential to enable fundamental software innovations, business strategies, and industries 4.0 to significantly enhance the quality of life and well-being of people all over the world through unmatched use cases that call for low latency, high real-time data communications, and enormous connectivity for cutting-edge applications that are designed for smartphones, home automation, intelligent buildings, driverless cars, and internet of things.

The downlink high throughput potential of 5G is 20 Gbps which offers dependable facilities for 4G WWWW, which stands for the 4th Generation of the Worldwide Wireless Web [24]. 5G is built on the Internet protocol version 6 protocol, and it enables users to have unrestricted internet access at their convenience, anytime, and anywhere using an enormously high-speed connection with maximum throughput at low delay.

Furthermore, 5G provides higher reliability and scalability to maintain enhanced energy-efficient wireless service telecommunications [25].

2.2.2. Internet of Things (IoT)

The Internet of Things (IoT) continues to play a pivotal role in facilitating the transition of traditional cities into smart ones by opening new channels for the collection of relevant data and information in a variety of formats. It is sometimes difficult to pinpoint the full impact of the Internet of Things (IoT) in smart cities and what it facilitates in detail. Nevertheless, the IoT's effects are seen and experienced in almost every facet of smart communities.

Therefore, IoT is fundamental to the realization of smart city initiatives since many smart cities' activities would be next to impossible without the development and widespread use of IoT devices in recent years. The goal of IoT is to facilitate the collection of data in both structured and unstructured forms in a wide variety of formats and through various methods. The deployment and installation of IoT devices form a network that collects data in a variety of ways to guarantee that the smart city has the necessary equipment to allow the interconnection that fuels the smartness of smart cities [10]. Devices like detectors, controllers, semiconductors, sensors, firmware, networks, middleware, actuators, and software make up the IoT ecosystem.

As a result of the IoT instrumentation, a wide variety of things, such as computer systems, mobile phones, wearable devices, households, buildings, edifices, automobiles, and power systems, can serve as data feeds in smart cities, allowing the rich diversity of data to be captured in different data types and from different data sources. The capabilities made possible by IoT devices are already ubiquitous.

IoT has sparked a revolution in what could be implemented in urban areas to render them more responsive to residents' needs and desires. The main benefits of using a wide variety of Internet of things devices are to gather data and engage with individuals in non-threatening physical interactions. IoT devices enable interactions with a relatively low cost, wide availability, and a simple setup.

The security problems associated with IoT devices may be broken down into two categories namely the physical layer and the technology layer security issues [68]. The security concerns related to the actual hardware of the IoT device and its physical location serving as points of interaction and data collection constitute the physical layer concerns.

The access, control, and permissions for the gathered data or the functioning of the IoT devices are all part of the technology layer's concerns. There are numerous IoT security-related concerns in smart cities because of these layers of concerns that require protection. These security concerns must be addressed and solved before people fully embrace the idea of smart cities as a place to live in peace and safety [26]. Many individuals may not agree to be videotaped or photographed in specific environments because of the lack of strong user data control methods and robust data privacy standards established in smart cities that govern the data collection and storage of different IoT devices (such as audio recorders) without raising privacy issues [26].

Another security-encouraged privacy concern that smart cities should tackle and appropriately find ways to cope with in the attempt to develop more privacy-aware smart cities [26] is the issue of archived data. It is essential to assess all the audio and video collections that have been captured, gathered, and archived over the years and find ways to delete them when not used.

There are security problems relative to places of data collection, where it is possible to acquire data from many individuals in one go even though only a single individual data is needed [26].

Many applications, systems, and technologies are being developed today in smart cities with the availability of IoT devices that produce privacy issues, such as motion detection, face recognition, sound recognition, biometrics acquisition, etc. For this reason, the technological security layer poses a greater data privacy threat; if a malicious user acquires control and access to the IoT device at the point of data collection, then the personal information of users may be exposed.

There is a plethora of suggested solutions to alleviate data privacy and security issues reared by IoT devices when evaluating the data information acquired at the data collection points. However, most solutions rarely get to the epicenter of data privacy issues, which are rooted in the criteria for data protection technologies that deployed IoT devices use in smart cities. The use of IoT devices in smart cities remains one of the most valuable assets because future smart city solutions will continue to depend heavily on the development and distribution of an abundance of IoT devices [26].

2.2.3. Information and Communication Technology (ICT)

To realize the goals of autonomous, efficient, and optimum processes and systems, many smart city solutions and innovations rely on information and communications technology [10] known as the ICT system. The connection between the Big Data ecosystem and the Internet of Things network in the entire smart city's infrastructure is made easier and possible by the ICT system, which opens opportunities for solutions to improve citizens' quality of life.

It is crucial to place ICT on par with the Internet of Things and Big Data ecosystems since it provides the necessary tools to translate and materialize data-driven decisions from data acquired through IoT devices. The Internet of Things (IoT) and information and communication technology (ICT) provide a framework for genuine public engagement, allowing for the introduction of positive, non-threatening change while maintaining familiarity and acceptance among the populace.

Information and communication technology (ICT) is the backbone of smart cities since it allows the widespread adoption and use of many advanced systems and technologies therein. In this context, one of the goals of information and communications technology (ICT) is to make it possible for people to connect and embrace various systems and technologies. Another goal of ICT is to make it easier for residents to provide feedback to technology providers and architects, with the end goal of ensuring that more effective ICT infrastructures are designed and deployed so that smart city initiatives may be implemented.

Due to its prevalence in enabling technologies, ICT plays a significant role in many smart city sectors. Nevertheless, ICT presents several security threats, since various systems in smart city environments are interconnected, mutually dependent, and exchange data with varying degrees of data protection. Security issues arise due to the interdependence of protocols and procedures inside the ICT network, as data transmission is performed in several different ways to aid the realization of decision-making that permits the quality of technologies and services in smart cities.

When there are breakdowns in connectivity or the impermissible exchange of personal data, individuals may become anxious about a wide range of security-related data privacy concerns. As a growing number of network technologies are created and utilized in ICT, it is obvious that there are security challenges and risks that must be addressed considering citizens' data privacy worries that may emerge due to purposeful or inadvertent compromission.

The frequency of geriatric health problems, public face recognition, and alterations to transportation systems are only a few of the data privacy concerns related to security vulnerabilities in ICT networks that smart cities must address [10][27]. There is no question that the existence of ICT in intelligent urban spaces is the fundamental facilitator of smart city connections and the major interface that engages with people to obtain information from them and deliver services to them.

2.2.4. Artificial Intelligence – AI

The smart cities initiatives rely on AI's ability to allow and support efficiency and optimization across practically all its processes and systems for a viable future. As the concept of smart cities evolves from one of conceptualization to one of actualization, artificial intelligence will play an increasingly important role in enabling all the linked components. AI makes it possible for innovative technologies to be developed, which in return boosts the appropriate strategies and optimization that are necessary throughout the operations of all smart city sectors [28].

To meet the current requirements of smart cities, several AI technologies are rapidly developing as potential solutions. These solutions include the realization of smart cities, the reward of clean and sustainable efforts, and the achievement of net-zero energy promises. Therefore, the growth of smart cities and artificial intelligence are becoming more intertwined now as Gartner's research [29] demonstrated in its 2018 projection that AI would become an essential component of thirty percent of all key-enabling smart cities' technologies by the year 2020.

This is a substantial rise from the past published 5 percent figure a few years ago. The influence of AI's dominance in 2022 can already be seen in the increasing deployment and enablement of autonomous technologies, such as autonomous cars, chatbots, telehealth, recommendation engines, etc. Artificial intelligence (AI) is becoming the not-so-secret ingredient that allows major energy suppliers to attain their minimal carbon dioxide CO_2 emissions to date, along with unrivaled efficiency and compelling profitability.

The ability of a city to function as a smart city is enabled by the collection and processing of huge amounts of data collected from a wide range of sources, including data from urban expansion, and the distribution of power down to enabling manual processes such as municipal services.

Developing and maintaining IoT sensors, equipment, and other technologies that are designed to promote the efficiency and environmental sustainability that is essential for smart cities is the bulk labor involved in enabling artificial intelligence. Changing the management strategy of a city's utility operations through data-driven solutions is one of the primary things that enables a city to become intelligent and more environmentally friendly.

In this area, artificial intelligence (AI) solutions have indeed made significant progress and are well on their way to governing problem-solving techniques to solve future utility’s operating concerns. The concern that is often raised is whether the utility system operation would function well with AI without major human assistance. Smart cities often investigate to facilitate the construction of robust systems that can operate independently over the long run.

Many company leaders are thrilled by the impact that cutting-edge innovations are indeed having on their industries, and the CEOs of artificial intelligence (AI) companies building software for the utility sector are eager to rise to the challenge and provide the missing link in the quest for sustainable growth.

The implementation of the Nvidia Metropolis platform, which makes use of advanced video analytics to improve the city’s services, transportation, and other relevant sectors [28], is a good example of how AI may be implemented to support the utilities of smart cities. This platform application aims to improve city services for both individuals and communities, strengthen cities’ infrastructures, and enable more sustainable cities that are consistent with Nvidia's mission. The platform collects data from a wide variety of sensors and other Internet of Things (IoT) devices located around the city to provide insights that may contribute to improving assets’ protection, supply planning, traffic management, and emergency response [28].

Likewise, a project led by Xcell Security House and Finance SA in Africa plans to enable the world's first intelligent AI-managed power station to better serve the continent of Africa by capitalizing on existing plant management knowledge and introducing new ways of doing business. This project is an excellent illustration of how AI may be used on a global scale to address some of the most difficult challenges that society is now confronted with.

This is a unique way to develop more intelligent cities in Africa by obviously driving the expansion of utility companies in West Africa, which may, in turn, assist improve other industries that rely on it. As the first effort to create and develop an AI-powered industry from the ground up, the purpose of this project is to employ cutting-edge sensor techniques and systems that integrate experience and expertise into every part of the operations of the power plant. If anything goes wrong, many stakeholders will have rapid access to operational data pertaining to the facility. The power plant environment will become much safer with more risk-mitigating protocols to enable more efficiency and productivity.

The potentials that artificial intelligence (AI) enables are virtually never-ending. The strength of artificial intelligence (AI) resides in its ability to coordinate processes and facilitate decision-making via the use of pattern recognition to deliver insights in data analytics and data science that enable the next sets of breakthroughs through the combination of software and hardware. In the process of making decisions, it is highly important to consider a hybrid cohabitation of both people and AI. AI can be implemented practically everywhere, from the most basic to the most complex of activities in smart cities.

AI can be depended upon especially when its deployments are faultless. Artificial intelligence is allowing cities to become smarter, which in turn allows their services and processes to become more streamlined and efficient. The more money that is invested in artificial intelligence, the smarter cities become, and ultimately the more people adopt AI. As more information is collected and evaluated, it becomes inevitable to leverage AI insights.

2.2.5. Blockchain

The industrialization of cities and their transformation into smart cities calls for a significant increase in the number of builders with different skill sets. For this reason, Software Architecture plays a crucial role in bringing about the new age of smart cities and meeting the sustainability needs of the near future [30]. This is accomplished by ensuring tech systems’ resilience during periods of demand ambiguity, inconsistency undependability.

Therefore, Blockchain is certainly one of the innovations that have the potential to improve not only the well-being of inhabitants in smart cities but also the standard of living in such communities. The term "blockchain" may seem or sound unfamiliar, but the notion of blockchain is easy to understand. Blockchain aims to facilitate transactions that are both visible and unchangeable to ensure data transparency and security.

2.2.5.1. What precisely is Blockchain?

A distributed digital ledger method, often known as the blockchain, is a technology or even a strategy that guarantees the record of transactions in a way that is public, enduring, and transparent. In the blockchain, the transaction record known as a ledger is only added to the chain of transaction interactions in the network. When a ledger is appended to the chain, the system ensures that only the addition of data is made and not the modification of any existing data in the chain.

The blockchain system is made possible by a mechanism that facilitates the formation of consensus between dispersed or distributed parties. These parties do not necessarily require the establishment of confidence in any other sense because they depend solely on the blockchain method to validate and document their general agreement [30]. The blockchain process has seven phases depicted in figure 3 below that make up the overall process a blockchain transaction takes from its inception through to its conclusion.

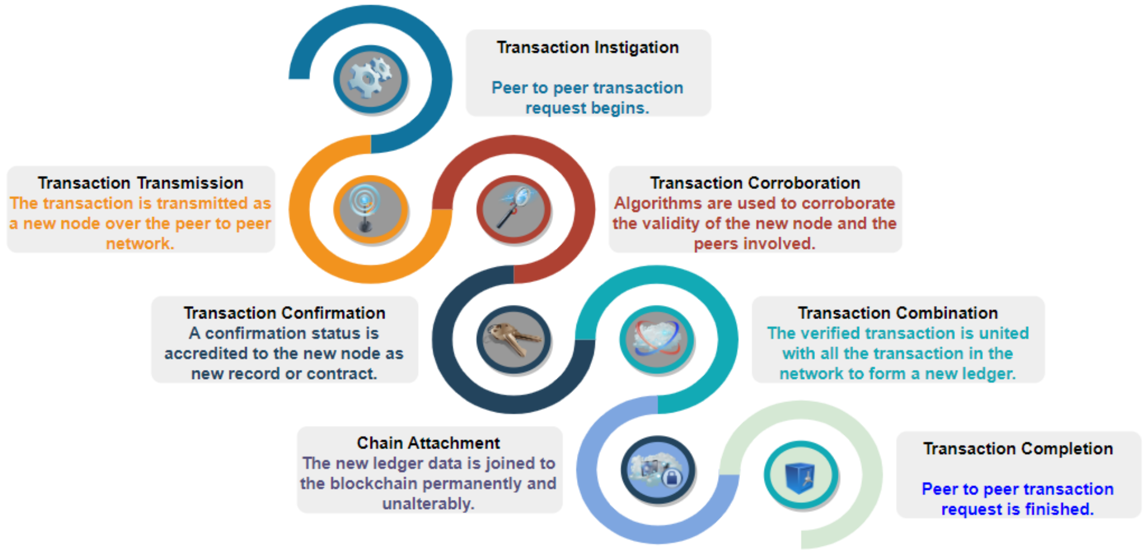

Transaction Instigation
Peer to peer transaction request begins.
Transaction Transmission
The transaction is transmitted as a new node over the peer to peer network.
Transaction Corroboration
Algorithms are used to corroborate the validity of the new node and the peers involved.
Transaction Confirmation
A confirmation status is accredited to the new node as new record or contract.
Transaction Combination
The verified transaction is united with all the transaction in the network to form a new ledger.
Chain Attachment
The new ledger data is joined to the blockchain permanently and unalterably.
Transaction Completion
Peer to peer transaction request is finished.

Figure 3: Blockchain Technology Process

As more and more tech applications are being created and implemented in smart cities, it is important to take note of the diverse products and use cases that are now making use of distributed ledger technology. Cryptocurrency is an example of an application of blockchain technology that may be seen in smart cities.

Because cryptocurrency is often regarded as the first practical use of blockchain technology, it remains one of the most fascinating use cases of blockchain. The fundamental premise of the cryptocurrency ecosystem is that no one actor or element in a network can successfully resolve a problem without the agreement of all other actors and components in the network. This is the challenge that underpins the cryptocurrency system. As a result, the blockchain process has an element of randomness that makes it impossible to manipulate it into accepting an entry in the ledger that other members dispute.

Everyone in the blockchain system has a copy of the data that is on the transaction network since that information is replicated across the network and disseminated to everyone on the network. Because of this, the ledger that is stored on the network is kept up to date, maintained, and thoroughly checked to guarantee that the changes are accurate. This approach makes it difficult to commit fraud or make alterations after the fact. The peer-to-peer networks are then continually updated for everyone when the revisions have been authorized, and each party is made aware of the ledger and holds a copy of all previous and present transactions [30].

The present privacy basis that has been defined in blockchain restricts access to data information to just those players participating in the transaction and trustworthy third parties. The need that all transactions be publicly broadcast presents a barrier to the implementation of different strategies for ensuring users' data privacy which is essential to overcome the mistrust of users. Despite this, it is still possible to protect one's privacy by preventing the flow of information to locations other than those intended and by keeping public keys in an anonymous location [30].

Members of the blockchain network community can infer that one person is sending a predetermined amount of money to another person even in the absence of information that would normally be required to make such a connection.

When most people think of blockchain, they still think of cryptocurrencies since bitcoin is the most prominent implemented example that is integrally related to blockchain technology. Consequently, many people still have the money euphoria from cryptocurrency.

Nevertheless, there are many additional advantages that may be gained from and made possible by blockchain technology. Blockchain is another wonderful tool for people, machines, and other entities to use in exchanging at scale, and it makes trading more dispersed and transparent. From a methodical standpoint, a blockchain is a terrific tool. There are many smart cities' potential applications of blockchain technology. Many aspects of smart cities, such as energy distribution and conservation, food and supply chain management, health care and real estate, and so on, may all make use of blockchain technology, which provides several advantages and applications that are discussed in this chapter.

When it comes to saving energy, there is a significant opportunity to harness blockchain technology to make the energy ecosystem even more trustworthy. Energy efficiency plays a significant role in smart cities; in fact, it is the engine that powers most innovations, as an increasing number of systems strive to operate as effectively as they possibly can. When looking at energy from a variety of angles, the energy landscape of smart cities comprises products and systems such as smart grids, electric automobiles, solar panels, and other similar technologies, in addition to many renewable energy sources.

Electric car batteries, for instance, may be seen as part of a larger distributed network architecture that enables most electric vehicles' features. By using by-direction methods, a smart city may provide the grid with surplus energy generated by its automobiles, stored in its batteries, and produced by its photovoltaic systems to relieve the smart energy grid of its burden. This smart energy network system can be implemented with blockchain technology. As cars connect to power sources to get energy, they can send excess electricity back to the electric grid. The photovoltaic cells and batteries found in individual homes may be thought of in the same way. Installing electromechanical systems in homes is critical to enable more automated and autonomous power generation, distribution, and storage of needed power in local banks while offloading surplus power to the grid's dispersed batteries.

In this scenario, the autonomous energy grid system is responsible for preserving the energy balance while also providing the required levels of efficiency and performance for the energy grid. The idea of creating a civilization that is both sustainable and efficient, one in which increasing amounts of renewable energy are collected and utilized to power the systems that are essential to our existence, is an intriguing one. Renewable energy makes all the difference and helps to alleviate the burden on the electric grid during times of high energy use or unfavorable weather conditions. It also offers the dependability that is required to meet the needs of future smart cities.

Considering the food sector, it is essential to keep in mind the number of occasions that e-coli outbreaks have taken place for example to better understand how blockchain could provide an alternative solution. This shows how vital it is to keep an eye on the food network and ensure that it is safe. Since the CDC was unable to determine which producer in the network was infected during the period of e-Coli outbreaks, they strongly recommended that food stores and people throw away their lettuces and get rid of other vegetables they had.

This specific use case serves to accentuate an opportunity where blockchain technology can be used. In smart cities equipped with a blockchain system that is integrated into their food delivery network, the problem of being unable to determine the source of an epidemic would not have occurred. The transparency and security of the ledgers are the two very significant features of blockchain technology. Assuming that farmers, food suppliers, and distribution partners are leveraging modern agricultural technologies to cultivate their crops, in this case, each small farmer in the integrated delivery system would have a method for storing all the details regarding their food production or providing food quality and safety thru a secure and trustworthy shared blockchain.

This would have been possible because precision agricultural technologies are used to produce crops. After the food-related epidemic took place, smart cities would have been able to read and obtain the blockchain of all food distribution transaction information with ease. This would determine precisely where and when the outbreak took place by using the documented ledger. It would instill confidence in the food supply chain while also supplying the researchers with the needed knowledge to fix and avoid any future problems relating to food quality.

In the supply chain sector as well, it is essential to investigate a further crucial benefit of blockchain, which is its ability to instill confidence in the underlying infrastructure. One of the problems that blockchain aims to answer is the age-old puzzle of whether one person can have faith in another even though they have never met or had the opportunity to get to know each other. The immutability of blockchain transactions and the certification of changes within the system to approve the ledgers make it particularly useful when doing business with an untrusted party.

Some nations have begun to accept or recognize cryptocurrencies as their legal money, while others are passing up the chance to obtain more information on the fundamental technology of blockchain. When distributed ledger technology is implemented into a city's supply chain, it boosts the legitimacy of transactions while also increasing their efficiency leading to the streamlining of the process that increases public confidence. For example, there are numerous supply-chain issues nowadays that may benefit from blockchain technology, particularly when it comes to the tracking of minerals and the distribution of resources.

One example of this is the mineral dispute over the columbite-tantalum deposit in the Democratic Republic of Congo. These resources are important in the production of electronic devices. Thus, the supply chain of these resources can significantly profit from blockchain technology. In this kind of supply chain, all stakeholders and crucial actors could be recognized, which would offer greater transparency for the mineral wealth. The existing supply chain often begins in the Congo (in Africa), continues via China (in Asia), and finally arrives in the United States of America (in America). Most contributors at the source are undisclosed.

All transactions involving the mineral along this supply chain, including its extraction and processing, would be tracked in an immutable distributed ledger accessible only to authorized parties. At the end of the process, customers will have complete faith that the electronics they purchased do not contain any minerals that were mined using forced or child labor. As a result, it is essential to highlight how the use of blockchain in supply chains improves society, finds solutions to many of its issues, and rebuilds public confidence in both interactions and transactions.

In the real estate sector, the advantages of blockchain technology can now be realized. Accountability, transparency, and integrity are important to allow what is referred to as smart contracts, and blockchain technology enables all three of these features. When buying a property, there are a lot of different people who need to be identified, notified, and have their information verified. This results in a lot of paperwork that must be completed. This procedure is very time-consuming, particularly considering the need of verifying each document that is involved. The inspection and validation of several legal papers are required throughout the residential real estate transaction process by all the parties involved.

When it comes to establishing and completing a closure on the properties, trust is of the utmost importance on all sides of the transaction, from the buyers and borrowers to the title firm and even the insurers. By using a blockchain-enabled shared ledger in a smart city, all relevant documents and parties to a transaction may be safely and transparently confirmed and added to a shared ledger.

When a property is allocated and passed to an interested party, the procedure becomes extremely simplified, and the processing time required to transfer the premises to other people is much decreased since all the information needed to complete the transfer is already confirmed and saved in the blockchain and distributed transaction. Therefore, the use of blockchain technology would assist in shortening the amount of time necessary to execute any additional transactions on the asset and enhancing the level of trust present throughout the process of purchasing real estate property.

When considering the advantages of blockchain in the healthcare sector, one of the areas in which blockchain gives endless potential is the healthcare industry. This potential extends from the viewpoint of public health to the interaction between a physician and their patient. The healthcare industry necessitates trust, transparency, and suitability to guarantee the well-being and life quality of patients as well as the personnel who provide care for them.

The existing covid-19 outbreak has stressed the health systems so people's faith and confidence in them have been compromised, making the healthcare industry a prime candidate for blockchain's enhancement of trust and accountability. Public faith in the system of health care has been shaken because of the Covid-19 outbreak, and it has highlighted difficulties in the healthcare system’s monitoring, transmission, and priorities that can be resolved by using blockchain technology because of the accountability of the information contained in the ledger.

Therefore, there is an opportunity to implement blockchain solutions into health service delivery to assist in relieving the strain placed on the traditional healthcare systems by the current pandemic [30]. Even if it may be difficult to deploy blockchain technology in healthcare, urban planners must work toward the incorporation of blockchain in the digitalization of healthcare systems. Only then can the public trust and faith be rebuilt in smart cities’ healthcare systems.

2.3. Tech Privacy Basis

The value of smart cities continues to showcase the enormous advantages that facilitate the realization of citizens' quality of life and well-being. The advantages that smart cities realize and enable continue to trigger the excitement of many people in hoping to live and experience them. Concurrently, many privacy-aware people living or wanting to live in smart cities are still anxious about the growing privacy risks linked with the core of the smart cities' promises. The essence of smart cities' possibilities resides in the generation and usage of data to empower urban technologies that deliver, to some extent, mutual value-added prospects for cities and their citizens.

The possibilities of smart cities reside predominantly on three mutually dependent dimensions, namely the collected information data type, the purpose for which data is being collected, and the value that the collected data enables. The three mutually dependent dimensions provide the foundation for perusing and assessing privacy concerns among citizens to enable successful privacy-aware smart cities.

The 3D privacy basis provides a clear avenue of the interrelationship that tech applications and systems in smart cities possess based on the three interdependent dimensions. The 3D privacy basis expands on prevailing citizens' privacy basis [6] and models [31] in literature to theorize when citizens or users are prospective to agree to use smart city technologies with privacy concerns; when they are further expected to agree to trade their data privacy under well-defined guidelines due to the perceived proposed value of services; and lastly when they are to be expected to object, reject and disregard smart city technologies altogether due to the value they attach and attribute to their data privacy.

The 3D privacy basis provides new ways of assessing how citizens' privacy is affected by various technologies. It boosts the adoption of new methodologies to practically help reduce citizens' privacy worries by instigating technology-specific sprightly guidelines based on several secured metrics that facilitate the practical and useful adoption of the framework in the smart cities space.

2.3.1. Framework Application Context

The realization of newer services and the improvement of existing services in enabling the smart cities initiatives are exceptional. The worth of data can no more be underrated in smart cities' spaces. The miracles of various technologies deployed in smart cities would not have been possible if the immense data collection effort was undermined. Data collection in smart cities does not just enable technologies, but it also increases myriad privacy issues when it possesses personally identifiable information that is not properly and securely collected, analyzed, stored, or deleted.

The various privacy issues spring from the identification of the type of data being collected and categorizing it as either personal data or impersonal data and associating the services the collected data enables to if the services are enabled with surveillance or without it [54]. The proposed value that the deployed technologies in smart cities provide via the services they enabled is critical in evaluating how citizens interact with them. The value must be appraised in consideration of citizens' data privacy tolerance given the proposed value. This is paramount to be able to empower and permit the formation of resilient smart cities where citizens are empowered with the necessary information and tools to better protect their data privacy.

A 2D framework model introduced earlier in literature by Zoonen [6] provided the model as an instrument to assist in the analysis and understanding of the way urban planners ought to incorporate citizens' privacy apprehensions in the preparation and construction of effective and required smart cities.

The diverse smart cities technologies must be assessed to provide a clear understanding to their users or citizens of what types of data the technologies used and determine whether the data is personal or impersonal, to ultimately ensure that the data is required to enable the specific technologies. The evaluation of the purpose of empowering services for citizens via technological solutions is critical in determining whether the provided services are realized with or without surveillance. The contemplation of citizens' feelings in smart cities is essential to deliver applied resolutions that riposte to the countless citizens' data privacy concerns.

The 3D privacy basis helps address the significance of understanding the value aspect of the data citizens provides to enable the technologies that facilitate services users benefit from. Thus, the interrelationship between data and technologies stands as a vital factor in defining whether the technology offers value in the context of smart cities mainly to citizens, cities, or both. A similar contrast is applicable even further by looking at whether the value provided by the enabled services is mostly for the public sector, private sector, or both, or even for the producers, consumers, or both, etc.

Considering the real provided value of deployed systems or technologies in smart cities aids in assessing and addressing citizens' privacy concerns by differentiating both the deliberate and inadvertent surveillance embedded in many proposed smart cities' services. The provision of better-valued services is critical and necessary when realized in a way that enables the active consideration of how personal data is used to empower services without allowing the deployed technologies to generate a surveillance state for citizens. The triumph of smart cities eventually depends on their ability to appropriately address, alleviate, and respond to citizens' questions, concerns, risks, and consequences pertaining to data privacy and security issues regardless of the wonderfully allowed technologies [32][33][34].

Incidentally, assessing every single technology deployed in smart cities for ways that contribute to citizens' privacy concerns is paramount. Zoonen [6] admonished the necessity to evaluate the kinds of technologies that are installed in smart cities with an emphasis on data collection and its purpose in the proposition of the 2D framework.

The 3D privacy basis augmented the benefit of the 2D framework in introducing the critical value dimension that retorts to whether citizens or cities are benefiting from the proposed value that the deployed technologies are enabling to justify their enablement in smart cities. The 3D privacy basis aims to provide answers to citizens' data privacy inquiries pertaining to installed technologies in sight of the value that the installed systems and technologies deliver to smart cities and their citizens to create buoyant privacy-conscious smart cities [31].

The 3D privacy basis comprises the data, purpose, and value dimensions that produce eight different operational spaces where smart city technologies or systems can be characterized after careful evaluation based on their data type, empowered services, and ultimately the value they provide to citizens, cities, or both. The real essence of the provided value can appear in different forms namely as security, health, monetary benefits, etc.

Eventually, the worth or benefit of specific technological systems in smart cities converges to a monetary value considering the need to justify the required investments necessary to create and deploy them. If the value produced by a specific technology or system profits mutually both smart cities and citizens, privacy concerns can be assessed through the data and purpose dimensions. However, if there is a conflict in the value proposition of the provided services pertaining to citizens or cities, then the 3D privacy basis provides the required premises to assess associated privacy concerns of the enabled services.

The evaluation may be in the form of an applicable agile directive procedure to set restrictions on how to handle the collected data and the techniques required to analyze the data to diminish the citizens' privacy concerns. The agile directive procedure deliberates data security characteristics and risks associated with technologies and systems being evaluated. It categorizes the evaluation outcomes on different privacy flags because there are data that are considered more private and sensitive than others by citizens. The agile directive procedure regulates how to alleviate or diminish the citizens' privacy apprehensions by setting guiding principles on private data storage duration as well as its expiration date and deletion time after service value enablement.

The 3D privacy basis augments its applications by considering the frequent dimensions (data and purpose) in research to provide an avenue for incorporating citizens' data privacy concerns in fueling technological data privacy solutions in tech applications. It is because people see certain personal data as more private and sensitive than others [6] and regard differently data privacy concerns based on the type of data collected and the profits they reap from it.

For instance, many users on social media do not care much about the data they publish online if they obtain the expected reply from followers [6]. The usefulness of the 3D privacy basis resides in the premise of understanding citizens' tradeoff between the tendency of forgoing data privacy and agreeing to personal data distribution in exchange for custom-made valued services that overshadow immediate data privacy concerns. This tradeoff is of the essence especially when personal data guidelines are implemented to diminish data privacy concerns.

2.3.2. 3D Privacy Basis

The 3D privacy context attributes privacy levels to all its operational spaces based on the number of five privacy dimensions [31] such as identity, query, location, footprint, and owner privacy operating in the operational spaces given the enabling technology or system. Identity privacy deals with the unauthorized release of a user's identity every time the user uses a smart city service. Query privacy deals with the protection of requests completed by users using smart city services.

Location privacy deals with the assurance of the protection of a user's physical location in using smart city services. Footprint privacy deals with the control and preservation of information that is recoverable or inferable from other microdata sets. Owner privacy deals with the protection of automated query computation from autonomous databases in attempts to access and get hold of personal information.

The 3D privacy basis associates the overall privacy level with privacy dimensions flagged by the technology and its data enablement.

Data privacy-enhanced technologies must be decided based on different privacy levels. The deployment decision of technologies and applications in smart cities should rely first on their provided value to citizens and the security procedures used to realize their purpose. The 3D privacy basis enables new assessment attributes for judging both current and future technologies in the smart cities space.

The 3D privacy basis facilitates adaptive technology assessment means for qualifying improved citizens' data privacy-conscious technologies founded on tech anticipated value and services. It eases a better method of scrutinizing the mandatory regulations that must be adopted to help decrease citizens' data privacy concerns. It enables therefore the adoption of more technologies that offer citizens value without threatening their data privacy.

The critical discrepancy of providing services is to ensure that there is a clear separation between services enabled with surveillance (designates surveillance) and those without surveillance (designates service). Strict and mandatory regulations are needed to decrease data privacy risks in some operational spaces. The practical mandate may require the deletion of personal data after service conclusion to eliminate added risks and damage to personal data used in authorizing the service.

Understanding the anticipated value that the tech application is enabling for citizens helps drive and influence the kinds of data privacy regulations needed for proper data protection and preservation. The 3D privacy basis simplifies data privacy deliberations in smart cities and provides a deterministic way of deciding whether the tech application is valuable and necessary enough to mandate the collection of private or confidential information to accomplish its purpose and deliver its value.

The eight different tech applications' operational spaces provided by the 3D privacy basis are boosted by the value dimension of technologies and are well subjugated by the association between the data collection type and the purpose of the application technology.

2.3.3. Framework Operational Spaces

The 3D privacy basis generalizes that any typical technology assessed can theoretically fall into one of its eight operational spaces. Only four operational spaces dealing with personal data are shown in figure 4 below because they deal with personal data.

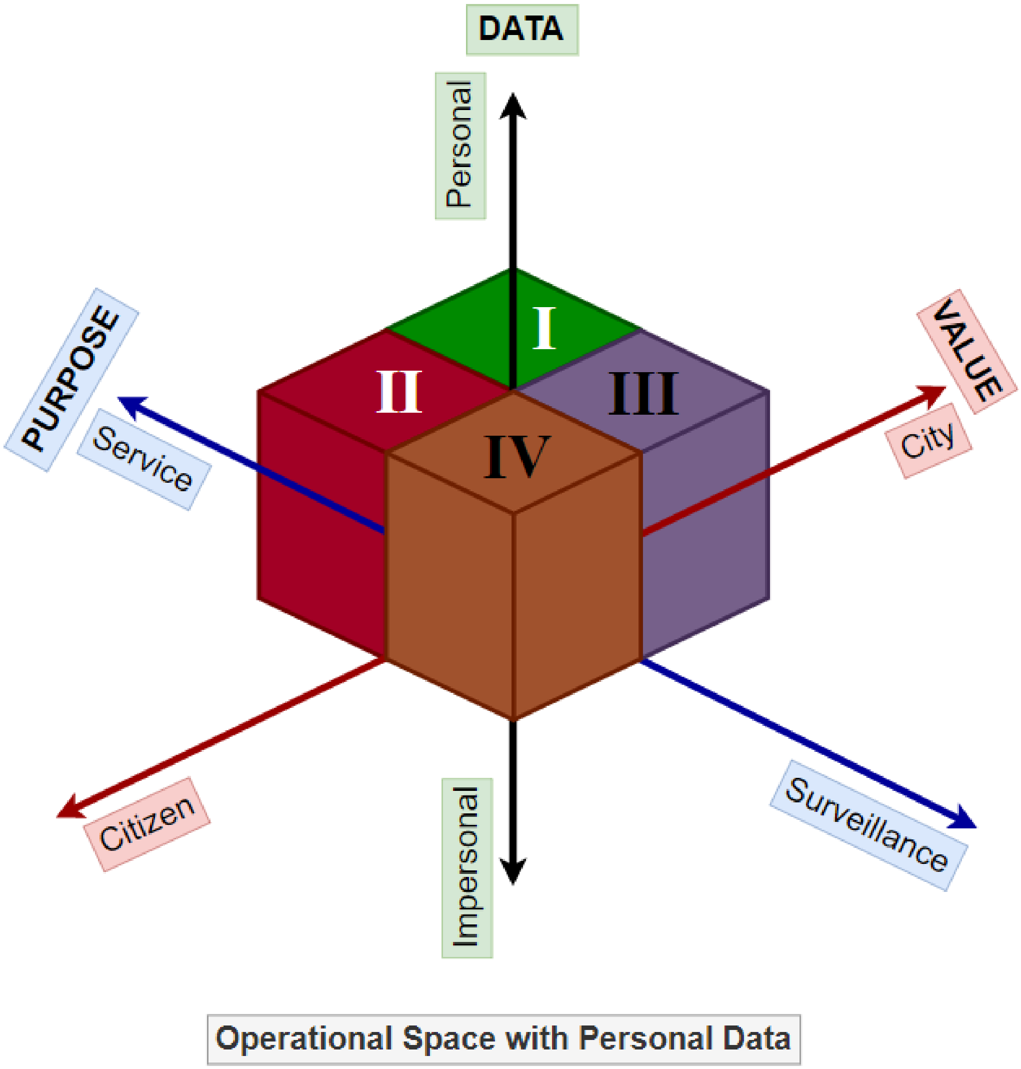


Figure 4: 3D Privacy Basis Dealing with Personal Data.

Several privacy concerns can be weighed against the provided value of the tech applications to citizens to determine the usefulness of collecting personal data to enable the services. If personal data is required to enable the needed and valued services by the citizens, then appropriate regulations must be adopted to avoid any potential data privacy risks considering the available technological protocols. The operational spaces pertaining to personal data are elaborated and discussed in detail in this section to help frame the discussion around the necessity of data privacy in the context of tech applications and systems in smart cities

2.3.3.1. Operational Space I

The operational space facilitates technologies and systems that deliver value mainly to the smart cities based on the service they empower while using citizens' personal data. In this operational space, the adoption of personal data from citizens enables technologies and applications that predominantly provide value to smart cities. The provided value may be enabled by using citizens' personal data in aggregation with other impersonal data collected in smart cities.

Many smart city technologies and systems are classified in this space such as most smart mobility tech applications that require more data containing a good representation of citizens' location and movement. Collecting the citizens' location and movement data is paramount to better plan and manage traffic via dynamic traffic light durations, non-congested routes, and enhanced transportation systems. Therefore, understanding the behavior of citizens and the culture in the city including citizens' movement is necessary for enabling an effective and active smart mobility system.

Understanding how citizens move around the smart cities and what means they employ for transportation provides improved ways to design, control, and improve city systems beyond contemplating only a single mode of transportation. For instance, if the tech application recognizes patterns of where citizens gravitate throughout their commutes at specific moments such as going to the beach on the weekends or to work during weekdays, the tech application in this operational space can use optimized algorithms to couple citizens' behavior with their location to better plan and align the optimized routes for their travel.

Further investment in tech applications that enhance citizens' experiences in smart cities can help improve citizens' participation in providing relevant information necessary to enhance smart cities' mobility systems and infrastructures. Mobility systems and infrastructures include road expansions and creations to accommodate and facilitate citizens' movement in smart cities.

The operational space one exhibits a high data privacy level since there is a significant potential to collect citizens' personal information that increases the possibilities of data privacy risks associated with personal data necessary to enable the tech applications proposed value. It is imperative to note that the purpose of the potential technologies in this operational space is mainly for services and not for surveillance.

There are no less than three of five privacy dimensions that are easily encountered in this operational space that enable the desired services for smart cities. Several examples of smart mobility technology systems and services are deliberated in [35][36] and expose potential privacy risks associated with enabling the services. There is a serious apprehension for location and query privacy risks in smart mobility technology [39] as many applications require the identification of location with a reference point that is associated with the identity of the user [37] or the IP address of the mobile device demanding the services.

Moreover, footprint privacy risks are also apparent with the incorporation of recommendations of users' optimal routes and inferences of mutual locations in users' requests and their service delivery.

For example, the sharing and urban mobility systems service [37][40] enable users to share commutes by optimally finding and providing an efficient multimodal convenient transport service value to users. It is obvious that query, location, identity, and footprint [39] privacy risks are apparent in this operational space. Thus, it is paramount in this operational space to mandate appropriate data privacy and security [38] regulatory protocols.

2.3.3.2. Operational Space II

In operational space two, the operational space facilitates technologies and systems that deliver value mainly to the citizens based on the service they empower while using citizens' personal data. Technologies that deliver value to citizens are critical even while using personal data in aggregation with some impersonal data to provide citizens with needed services.

These kinds of technologies should be encouraged and invested in to better protect the personal data that they utilized to enable their services. It is obvious to associate this operational space with technologies that offer services to citizens due to mainly the collection of personal data. If personal data collection is prevented, some of the technologies in this operational space will become rather useless or not relevant to enable the value proposition of their services.

The widespread presence of smart health systems and technologies resides in this operational space where citizens receive tech-valued services from real-time notification of potential danger zones or health crises that they need to address or distance themselves from. Smart health technologies use personal data from citizens predominantly citizens' health history and background information together with their pedigree to efficiently predict and recommend safe practices and measures for people to assume and follow for a better health outcome.

The expected value of technologies and systems in this operational space is directed more toward the well-being of citizens although smart cities participate in the infrastructure build-out to provision and enable the collection of data and its analysis to better connect medical health experts with citizens. The smart technologies and systems in operational space two empower health experts to detect and predict associated health patterns rapidly in affected patients.

Many smart health tech applications would be impossible without the collection of personal data and the insights drawn from personal data [41]. The provided value of health benefits affords citizens a plausible trade-off opportunity to better evaluate the benefits between the potential data privacy and security risks with the probably anticipated health benefits.

If the anticipated health benefits or value of the smart health tech application dominates and outweighs the potential data privacy and security risks, dedicated efforts must be made to find ways to control the smart health tech applications data, grant the ownership of the health data to the individuals it corresponds to, and determine an avenue that simplifies the acceptance of similar smart health technologies.

Operational space two is considered a high privacy level operational space because there are many potential data privacy risks associated with the personal data being collected to enable the technologies in this space even when the purpose of the services provided by the technologies is not deemed for citizens' surveillance in any way, shape, or form. It is apparent that many data privacy risks can be experienced in this operational space in attempting to enable necessary services for citizens. For example, the e-Health tech application that offers medical services to patients such as prescription refills utilizes their formerly kept database of patients' health record to simplify and optimize the health service provisioning [33].

Smart health tech applications in this space present high apprehensions for identity, query, and owner privacy concerns [41][42][43] by requiring the identification and authentication of the beneficiary of the services in the query requests. The beneficiary's personal information is accessible in the database by the query request whenever there is a significant match that accurately enables the provision of required services.

In this operational space, attention needs to be placed on the essential demand for proper data analysis before any attempt to update database information. The process of updating database information must be securely and reliably completed to enable suitable and correct servicing of patients [41].

Otherwise, the smart health tech applications would be a catastrophe whenever information is compromised. Thus, tech applications in this operational space must mandate a proper security protocol and regulation procedures [44] to reduce citizens' data privacy risks associated with potential enabling technologies [45].

2.3.3.3. Operational Space III

Operational space three facilitates technologies and systems that deliver value principally to smart cities by enabling surveillance systems that use citizens' personal data in aggregation with some impersonal data. Many smart city management and security systems are more ubiquitous and prevalent in this operational space to facilitate the secure operation of smart cities and guarantee systems safety. Most of these tech application systems are created to anticipate and address security risks within smart cities with their collection, possession, and processing of citizens' personal information [46] to associate the information with citizens' moves through the continuous collection of video footage feeds of alleged citizens [47].

In this operation space, it is evident that citizens' personal data is collected, various representations of artificial intelligence models are deployed, several machine learning models dealing with facial recognition of citizens' image feeds are established, and constant real-time video observation systems are operated to enable nonviolent smart cities [48]. Many tech applications in this space are intended to allow quicker information broadcast for faster security interventions.

Many smart technologies operating in this operational space are generally found to serve law enforcement [49]. They significantly profit the law enforcement sector with the provision of evidence through the collection of real-time citizens' personal data [48] aiding in tracking their locations and movements. These tech application solutions enable better and more secure smart cities through the deployment of more law enforcement systems in areas associated with higher crime rates or areas comprising many people with criminal backgrounds.

Due to the great potential of citizens' surveillance, this operational space possesses the highest level of data privacy concerns because citizens' personal data is collected by government entities sometimes without citizens' awareness and consent to enable services that do not benefit them primarily. In fact, some citizens are uncomfortable knowing that they are being tracked and can be potential suspects in any investigation should their data fit a prescribed profile of a potential suspect. The potential privacy risks associated with the various technologies used in this operational space coupled with the surveillance intent of the technologies can not be underestimated. It is obvious that many of the five privacy dimension apprehensions are concurrently reflected in the enablement of smart city surveillance services.

Knowledge in crime prevention using video surveillance technologies [6] encompasses the wide-ranging identification of people and following people's movements through unified surveillance data feeds obtained from numerous IoT data feeds. For instance, all five privacy dimensions are apparent in crime prevention systems, and the interconnectedness of privacy dimensions produces a higher privacy risk level that must be appropriately controlled.

The identity, query, location, footprint, and owner privacy fears [47] [48] cannot be exaggerated in the collection, processing, and analysis of real-time video data feeds to perceive, predict, and anticipate an explicit action necessary to initiate a striking retort [49][50].

2.3.3.4. Operational Space IV

Operational space four facilitates technologies and systems that deliver value principally to citizens that are enabled by surveillance systems that use citizens' personal data in aggregation with some impersonal data. In this operation space, there is a great presence of many smart governance technologies because these systems and applications allow more engagement between cities and citizens to guarantee that cities are providing citizens more value by knowing their interests and feedback. Simultaneously, the tech applications and systems in this space simplify both the communication and interaction between citizens and cities over a reiterative procedure of systems enhancement. This operational space encourages the development of technologies that solidify the interaction of both citizens and cities in many different forms regardless of what data is collected and used.

There are various potential benefits and advantages in enabling surveillance services for citizens to facilitate the enhancement of security, safety, and overall credibility of smart cities' systems and applications. In this operational space, there seems to be a paradoxical effect in the possibility of potentially having citizens monitor government management, interventions, and organizations to control how effectively they process collected data and deliver anticipated services [49][50].

Due to possible citizens' surveillance, this operational space possesses the highest level of data privacy concerns because citizens' personal data may be collected without their awareness or consent to some extent with the goal of surveilling them. Citizens may not mind if there is no direct impact on them, but if they are affected and find themselves confronted with the evidence of personal data collected from them without their conscious consent, then their attitude toward these technologies may completely change. Some smart governance technologies examples are conversed in [51][52] to depict the probable and active privacy dimensions necessary to facilitate the surveillance of citizens and measure the citizens' acceptance or rejection level of a provided service.

Respectable citizens' governance necessitates the involvement of citizens in providing criticisms and expressing concerns about what matters to them. It is paramount in enabling these smart governance technologies that proper citizens' authentication mechanisms [52] be in place together with a reliable security protocol in all necessary interactions between citizens and smart cities' tech systems to avoid breaches and eliminate any misrepresentations.

The query, location, identity, and owner privacy dimensions are overriding in this operational space, with the inclusion of footprint privacy dimensions when considering surveillance needs. Henceforth, there is a bigger requirement to properly assess and address privacy and security risks and issues in this space [49] through a definite set of guidelines pertaining to personal data collection and use for greater value and citizens' benefits.

2.3.4. Tech Privacy Basis Significance

The essence of the 3D privacy basis is to respond to two essential questions pertaining to data privacy concerns in smart cities considering the deployment of myriad tech applications. Primarily, the 3D privacy basis focuses on the assessment of numerous prevailing technologies installed in smart cities that use citizens' personal information to enable services and values that benefit mainly citizens.

By the way, the 3D privacy basis evaluates the surveillance capability of technologies by evaluating the kinds of data collected and used to enable them, and the data handling techniques that are necessary to realize and enable valued services. Therefore, it guarantees that citizens' personal data inspire decisions that benefit citizens and safeguards appropriate regulations for data obliteration after the service completion to eliminate the further use of data for other purposes.

Citizens are prepared to trade some personal data in return for valuable services that benefit them. The case of Saudi Arabia [78] highlighted people's tendencies to overlook privacy concerns for some necessary benefits. Furthermore, the 3D privacy basis deliberates technologies that offer value through the services they enabled to both cities and citizens.

The serious issue that the 3D privacy basis highlights are the necessity to store and accumulate more personal data to identify patterns and build trends as citizens' and smart cities' needs change. For instance, controlling and reducing traffic jam to enable citizens' mobility in smart cities involve optimization over time to incorporate specific times citizens prefer to move based on their needs.

The citizens' behavioral patterns and trends in their commutes are important to consider in enabling better and more efficient management of citizens' mobility and migration. This is critical to guarantee that citizens profit from saving on commute time, especially in conditions of traffic with bad air quality. It allows smart cities to deal with lower gas emissions from cars given cars are spending less time on the roads.

Therefore, the 3D privacy basis help informs whether and when citizens are prospective to accept enabling technologies with their private data to receive valued services even if they must give up on their personal data and share data ownership to some extent. Many people can hardly remember sites and tech applications where they shared their data or consented.

The research question that the 3D privacy basis deliberates on is whether citizens' privacy concerns would diminish if and only if the value that technologies enabled through services were meant for citizens only, or in major part for both citizens and cities. A similar question could be asked if citizens are prospective to accept trading personal data for services enabled by technologies that offer value to them only, or to both them and the city.

The case of Saudi Arabia [78] demonstrated the citizens' tendency to gravitate toward the acceptance of valued services for their benefit. This tendency leads citizens to overlook potential data privacy concerns to acquire the proposed valued services enabled by technologies. The 3D privacy basis pursues to highlight the various factors that can influence and affect citizens in selecting anticipated valued service over data privacy concerns and shade lights on when it is appropriate to efficiently assess upcoming technologies and systems.

Secondly, the 3D privacy basis pursues to comprehend and highlight the value that technologies enabled with personal data provide to citizens and cities to help identify and assess whether there are ways to provide the same value with technologies while using impersonal data. The idea to substitute technologies that use personal data with those that use impersonal data while providing the same or equivalent services and value to both cities and citizens is a great driver toward more privacy-aware smart cities.

The real problem is knowing and understanding how to impersonalize technologies that use personal data and still provide the same value to both the citizens and the cities. This pertinent question and endeavor would offer an opportune method to recognize how to expand technologies that use impersonal data to meet the standard mandate of those technologies that use personal data.

A qualitative tech data privacy survey enhanced the literature's findings [78] to reflect indeed the tendency of citizens to overlook their data privacy concerns in return to receive valued services from tech applications. The insights and observations from the privacy responses demonstrated the willingness of citizens adoption of tech application services that provide value to them. The privacy concerns associated with technologies assessed by the 3D privacy basis typically apply to technologies that use personal data to enable value through services to citizens or through surveillance of citizens in smart cities as depicted in Table 1 below.

Data	Purpose	Value	Operational space	Privacy Level	Technology/System
Personal	Service	City	I	High	Smart Mobility Smart Economy
		Citizen	II	High	Smart Health Smart Education
	Surveillance	City	III	Highest	Smart Government E-Government
		Citizen	IV	Highest	Smart Governance Citizen engagement

Table 1: Personal Data Tech Operational Space Privacy Levels

The privacy concerns resulting from the use of citizens' personal data for their surveillance are detrimental to citizens and affect their adoption of potential future technologies. The inquiry to riposte is whether citizens' data privacy concerns diminish if the tech applications only provide value to citizens and grant citizens control over their personal data.

2.3.4.1. Framework Inference

The issues pertaining to citizens' data privacy in smart cities will remain a key decider for resilient and effective privacy-aware smart cities. It is paramount to constantly evaluate the data privacy worries of each technology in smart cities to guarantee that there are no violations of the citizens' data privacy rights while realizing tech innovations and enabling tech-intended values. The essence of the five privacy dimensions can differ across people and contexts due to cultural and geolocation implications.

In doing this work, a tech application data privacy survey was conducted to explore mainly students from Arizona State University in the United States on their views of data privacy use in tech applications to help understand their data sharing tendencies in using tech applications. More research should expand on the 3D model with more quantitative data from citizens' surveys in various geolocations to determine how people of different demography and background balance the five privacy dimensions namely the location, query, identity, footprint, and owner privacy. The 3D privacy basis remains the relevant avenue to evaluate both existing technologies and qualifying forthcoming deployable technologies because of citizens' data privacy considerations over the envisioned tech-enabled value.

It is indispensable to certify all deployed technologies in smart cities through thorough assessment and validation to guarantee that there is no violation of users' privacy rights for either users living in smart cities or using tech applications. The 3D privacy basis sprightly and dynamic tactic of judging technologies that use personal data in smart cities based on what citizens consider confidential is necessary to ensure tech application makers deploy solutions that do not generate serious data privacy problems in the long run.

Simultaneously, it enables a path for citizens to ponder the benefit of providing and trading personal information to obtain valuable services controlled by the mandate of agile guidelines and policies before technology deployments.

CHAPTER 3

DATA PRIVACY AND SECURITY

3.1. Smart Cities Data Envelop

3.1.1. Data Composition

Data is the lifeblood of a smart city, and the capacity to make many data-driven choices is crucial to the smooth running of a city that strives to meet the needs of its residents. It is necessary to have methods for monitoring the allocation of resources among residents and ensuring that improved services are supplied to them in a manner that is efficient and optimized. The success of smart city programs depends on the continued collection and analysis of data from residents, homes, and communities. This data may be either anonymous or identifiable. Data on road transport, climate change, cultural events, social events, parking, library events, and other integrated service activities, as well as data on pollutants and air quality, are examples of impersonal data gathered by large smart cities. Data has a very significant influence on practically every aspect of smart cities, including transportation, health care, public safety, budget management, quality of life, privacy, and welfare, to name just a few.

Data in smart cities is a glimmer of hope for all elements of smart cities since there is a need to comprehend the internal workings of smart city management to find gaps and areas that must be improved. Automatic monitoring IoT devices are necessary to guarantee that optimization outcomes are implemented as more data-driven choices are made and executed through services provided by smart cities technologies in many areas requiring upgrades and improvement. The way the data is gathered must be adequate to guarantee that the data is collected from real events. This is necessary to ascribe some meaning to the collected data and determine how it might be utilized. Many different representations of things, processes, people, and devices can be found in smart cities. These characterizations can be found through the data that has been collected in the interconnectivity of the telecommunication networks that make up the digital artifacts that are found in smart cities.

The data ecosystem of a smart city includes technologies for data collection, such as sensors; tools for data storage, such as databases; tools for data analysis, such as cloud software; and mechanisms for data protection, such as cybersecurity infrastructures that encrypt the data. The relationship between the collection of authentic data and the analysis of that data gives birth to a type of data known as generated data, which offers smart cities insights and values. In smart cities, many sources of data come from cloud computing, deployed IoT devices, crowdsourcing, the internet, social networking sites, handheld platforms, smart cards, automobiles, databases, etc.

People have a natural curiosity about how both public and private information are managed, and as a result, the subject of how this data should be categorized becomes more important. The issue pertaining to the quality of information is another frequent worry in smart cities. It is not the fact that data are gathered that makes them useful. Sometimes data needs time and resources to clean up the data before doing data analysis to anticipate any useful insights behind the collected data.

Data collection from people, homes, and communities, all part of the smart city's data workflow that ultimately forms the ecology of the data acquired in smart cities, is a source of worry when it comes to optimizing the smart cities’ operations. Most of the data acquired from people are information obtained through smartphones and mobile devices that are affiliated with them. This data is essential for associating a person's mobility with their preferences through their pursuits. This is accomplished by determining the services and activities that a person engages in the most, as well as the things and occasions to which they respond most of the time.

Mobile devices capture a wide variety of data, which if properly analyzed, may offer a more accurate depiction of an individual's level of interest in almost all activities that are carried out. For instance, mobility data may be acquired from people and offer some tracking of the individual based on the sites they interact with or the areas they are present in, as well as the method of transportation.

The data for the queries may be gathered through numerous purchases that an individual makes, the streaming movies, soaps, or programs that the individual watches, the time of day and the day of the week that they watch them, and so on. Personal health data may also be recorded when an individual possesses a smart eHealth application that tracks health patterns and activities and enables suggestions and recommendations.

Utility services, electricity, and energy consumptions produce a lot of information about households, which may be used to control traffic and presence inside the houses, and more significantly, the number of resources that are required to fulfill the requirements of the households.

Numerous data are gathered for each home, and these data show the amount of energy and power that is required, as well as, more crucially, the time of day during which the power need is greatest. For instance, the times and days when the houses are full of people would result in an increased demand for energy and electricity, as well as a higher need for water to meet the people’s requirements. Therefore, smart cities can gauge the typical amount of energy and water a family may consume by looking at how much demand there is for certain services at various times of the day.

Individual activities may be effectively linked to smart home performance thanks to data gathered from connected smart devices and the internet, ensuring that no wasted energy is generated and that each home receives just the right amount of power to meet its needs. Advanced devices in homes provide convenience and efficiency by guaranteeing, for instance, that lights are turned off when the area is not occupied by using technologies that leverage motion sensors. When smart home gadgets are networked and communicate with one another through the internet, there is a higher chance of learning about the inner workings of individual houses and using those insights to fine-tune the energy consumption and provision of services.

Communities' data is gathered in a similar fashion, considering the technologies that are realistically implemented and used in each community. The end goal of interacting with community data is to improve the quality of goods and services offered to its residents. Just as people's data feeds into household data, so is household data feeding into community data. As a result, the gathering of many household data is integrated and joined to produce what is known as community data.

Information on the local social and cultural complexities may be readily gathered by studying community data's noticeable features. Most of the data pertaining to the communities are trends in aggregated data, which IoT devices installed in the communities collect to keep track of the internal dynamics of local services and how people interact with them.

For instance, data from cameras that are installed in neighborhoods as well as at traffic intersections are equipped to record habits and patterns in the community. Body cameras are worn by law enforcement officers and other patrolling personnel in a neighborhood to record various encounters of people's conduct and attitude. Other examples include the fact that statistics on a town's air quality and noise level may provide an indication of the many health-related issues and concerns that are prominent in the neighborhood and prevent people that they may be at risk of experiencing some related sicknesses.
Likewise, data that is gathered in communities give insights into the events and activities that people who live in those communities tend to gravitate depending on what is going on in the communities at the time and days that those activities and events are taking place.

These insights give further advice to the communities to better prepare in serving the demands of their inhabitants by offering them the protection and safety they need while moving from one site to another. These insights are helpful to communities in planning for the effective deployment of security personnel, for enough transit and parking means, as well as meeting the needs for electricity and power. As a result, the data that are gathered in communities give insights that describe the characteristics of the residents that live in such communities.

These insights also highlight the priorities that should be considered to satisfy the expectations of the inhabitants. To stand a chance of living up to and exceeding the requirements of their citizens, most smart cities are prepared to invest in expanding the number of insights that can be garnered from the data that has been collected.

Smart cities' data process may be depended upon to help identify the areas that should be targeted and invested in to improve the quality of life and wellness of inhabitants when more community data are gathered inside a city and patterns are identified to accentuate the requirements and desires of each neighborhood within the smart cities.

Insights are generated after clear data analysis has been performed on clean data acquired from residents, homes, and communities to favorably affect the operations and services of smart cities. Figure 5 below illustrates what may be included in the data-gathering ecosystem of smart cities with every data source interconnected to enable the Big Data ecosystem for smart cities.

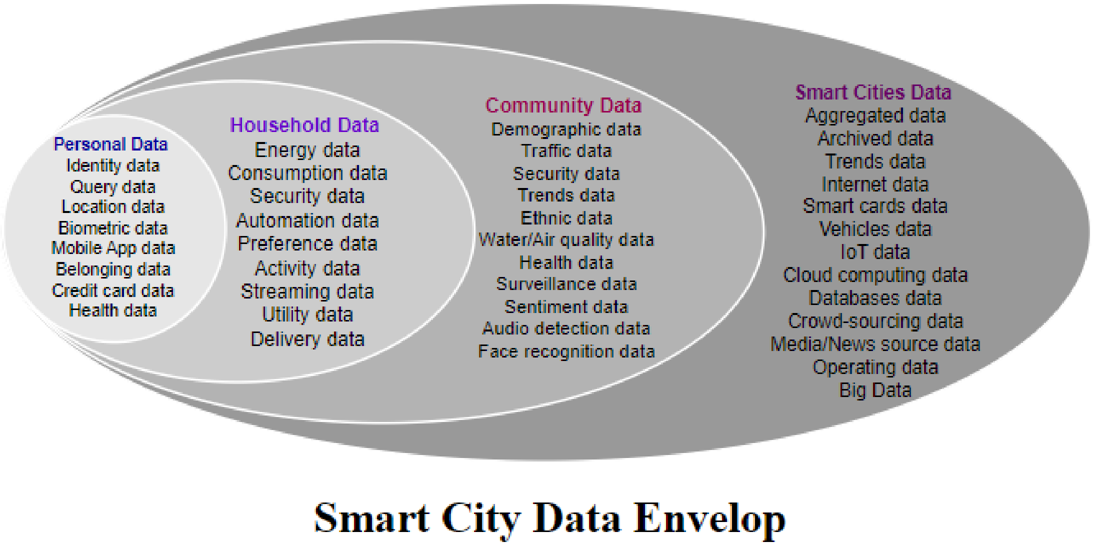


Figure 5: Smart City Data Envelop

There are several security and privacy issues connected to data, which arise whenever data is gathered, analyzed, processed, stored, or archived. Smart cities have faced the ultimate challenge of safeguarding and maintaining the privacy and security of their people's personal information while simultaneously improving their services and operations to guarantee that all risks are minimized appropriately. These are the questions that must be answered to make it possible for residents to participate in a variety of smart city activities.

3.1.2. Big Data

Big Data is an umbrella term that refers to the process of handling and organizing massive and complex amounts of different kinds of data that are generated through various avenues such as data captured through the plethora of IoT devices that are installed in smart cities. Big Data comprises data that is captured from IoT devices from various sources. Big Data refers to all forms of data, both organized and unorganized, that need to be stored, analyzed, used, and disposed of.

Having a large volume of data to analyze for tech applications and store for trends and patterns always raises several challenges and concerns, particularly when dealing with sensitive personal information. To allow more privacy-aware smart cities, it is necessary to solve the myriad of security and privacy problems that crop up during data collection, processing, and storage. Big Data entails the collection and storage of more than 2.5 quintillion bytes [10] of data every day, and most of this data contains private and sensitive information from individuals who may have not given their permission for it to be gathered and kept.

Whenever data or the platforms that store personal information are hacked, privacy concerns arise especially when data was acquired and taped into without the owner's authorization [53][27]. When the information at hand is personal, people must ensure that their data as well as the equipment that handles, retain, and gets rid of it are properly protected. When individuals perceive that their personal information may have been exposed due to a security flaw or breach, they naturally become concerned about their right to data privacy.

For example, if personal data was not captured, processed, and retained, people would not have to worry about their personal information being misused, and would care less about data security implications. Data communication and exchange between systems are vulnerable to interception, which may lead to data theft and the disclosure of sensitive information. Information processing security mechanisms may be breached if systems are not protected during analysis or if data is examined using untrusted third-party software. When data is kept on systems or mobile devices that may be replicated and hacked, it is at risk of being stolen and used maliciously.

With so many unknowns, privacy-conscious smart cities must find solutions to the various security-related data privacy issues associated with Big Data. Unlocking Big Data's full potential will allow even more value to be realized in smart cities via the use of cutting-edge algorithms and data analysis tools that make it possible to retrieve relevant information. However, this must be done in a secure and private manner that respects the data privacy of citizens [10][54].

Atmospheric data, phone logs, genetic data, e-commerce information, internet search indexes, medical files, military records, picture libraries, radio frequency identification data, surveillance footage, social media archives, video libraries, and weblogs are all constituents of Big Data [10]. The sensitive nature of personal data raises several security-induced privacy problems if it is compromised, as shown by the preceding cases.

3.2. Security-Induced Privacy Issues

The Internet of Things (IoT) is a crucial component of smart city infrastructures. The Internet of Things makes it possible to gather data and interpret information, which benefits both local authorities and residents. Many useful tech applications are made possible by the widespread deployment of IoT devices in smart cities which come with their own set of data security risks. Because of potential disruptions of information and data flow, IoT security vulnerabilities cause additional privacy concerns for residents and users. Security challenges associated with the Internet of Things (IoT), Big Data, and information and communications technology (ICT) empowered applications generate several data privacy-related vulnerabilities in smart cities, which must be well understood to construct resilient privacy-aware smart cities.

This chapter gives a thorough, categorized, and broad overview of data privacy concerns arising from the Internet of Things (IoT), Big Data, and Information and Communication Technology (ICT) empowered tech platforms and their inherent security problems; and it offers remedies in the context of the appropriate citizen value-oriented privacy basis operational space [54]. The basis of the classification of different tech applications is determined based on the application’s most pertinent privacy basis operational space, its applicable security issues, and the current remedies available to alleviate the related data privacy concerns among people in smart cities.

The world's main cities must evolve from "cities" to "smart cities" to keep up with the rapid increase of their urban populations. This matters because of the difficulties brought on by the urban sprawl because of people moving from rural areas to cities in search of better access to services and opportunities. Automation, optimization, and performance are essential for managing the operations of smart cities at the speed and dependability required to meet the needs of citizens when it comes to the delivery of services and opportunities.

The technical revolution of smart cities enables these solutions to fulfill the current and future demands of smart cities to guarantee the flourishment of citizens' well-being and quality of life. These innovation breakthroughs and progress are made possible because of the IoT ecosystem, Big Data, and ICT bases. Smart cities are being radically reshaped by smart technologies and systems that are deployed to engage with citizens, as people discover ever more creative ways to accept and use these innovations.

Today's smart cities are founded on the IoT, Big Data, and ICT frameworks, which raise the prospect of having efficient, optimal, and practically applicable smart cities that address citizens' needs of provision, consumption, and management of demands and services. However, real smart cities constructed only on IoT, Big Data, and ICT frameworks have shown some lack of effectiveness, not because of the issues and problems they are solving and addressing, but rather due to additional issues and problems they are causing and generating for citizens. These additional issues may be even more detrimental to citizens to the point where they can choose to forgo the benefits of the deployed tech applications.

The security and privacy issues that the IoT, Big Data, and ICT frameworks engender are often more important to address for the average citizen than the original ones they are designed to address. The Internet of Things (IoT), Big Data, and Information and Communication Technology (ICT) frameworks all contribute to new problems, including concerns over personal information theft, network safety, and data ownership. Concerns about tech applications' effectiveness highlight and center on problems that have direct and lasting consequences for the public.

Because data privacy and security are concerns shared by city residents, they must be well-thought-out and resolved before many more issues associated with IoT, Big Data, and ICT-enabled technology applications arise. It is paramount to address these issues immediately when dealing with each framework rather than addressing these issues at the point of convergence where the three frameworks that make up smart cities contribute to the overall issue in various ways and forms.

More progress has been made in Big Data thanks to the proliferation of IoT devices and systems, which have made it possible to collect a wide variety of data in large quantities leading to unlocking valuable insights through effective data analysis. The most valuable aspect of a smart city is the ability of its information and communication technology systems to process data to benefit the city and its citizens. Many useful applications have been made possible by the widespread availability of IoT devices in so-called "smart cities," but these advancements have also led to a slew of security concerns.

Because of these security flaws, the transmission of information and data within the ecosystem of ubiquitous computing is disrupted, which in turn raises additional questions and concerns surrounding the tech applications' users' and citizens' right to personal data privacy.

As a result, it is crucial to evaluate, comprehend, and reassess the security and privacy problems raised by IoT, Big Data, and Information communication technology paradigms about the tech applications and systems they empower to create viable smart cities. The 3D citizen value-motivated model [54] recommends the development of citizen privacy-aware smart cities as a means of ensuring the successful implementation of smart cities. Smart cities must therefore be developed in a manner that maintains the safety and confidentiality of its citizens' data before they can be considered effectively smart. Based on the most significant operational privacy space of the tech application [54], this chapter intends to provide a synopsis of the various security-generated data privacy challenges and some corresponding current and prospective solutions that emerge in research through the collaboration of IoT, Big Data, and ICT paradigms in the deployment of connected smart city technologies. Several smart cities' applications, platforms, and technologies originating from the Internet of Things, Big Data, and information and communication technology present various security-made privacy risks that are characterized to demonstrate the applicability of the 3D privacy basis and the possible solutions available to mitigate the associated concerns.

3.2.1. Smart Cities Technologies

There are numerous technologies for smart cities that may be taken into consideration when evaluating security-induced privacy problems in all areas of life in smart cities. However, further effort is necessary to properly handle these data privacy challenges if privacy-aware smart cities must be realized. It is essential to take precautions to guarantee that the technology solutions and the infrastructures that are used to drive smart cities maintain the confidentiality of personal data during all interconnections, correspondence, and network communications while carrying out or delivering services. As a result, this work addresses four broad technologies that are facilitating smart cities today, along with some of the accompanying systems that are supported by the Internet of

Things, Big Data, and Information communication technology infrastructures, all of which are venues whereby various privacy and security problems are encountered. The terms "smart mobility and transportation," "smart energy," "smart health," and "smart governance" each refer to a specific technology that is discussed.

3.2.1.1. Mobility and transportation in smart city

Technology that enables smart mobility and transportation is becoming more prevalent in smart cities, and it serves an important part in the process of making cities intelligent. It is very difficult, if not inconceivable, for a city to be deemed smart where there are no efforts in place to tackle the mobility and transportation concerns and requirements of its citizens. It is because transportation problems are one of the primary causes that create problems and needs in many smart cities.

The migration of individuals from rural regions to urban areas is primarily made easier by the creation of pathways that make it easier for people to move about and go from one place to another. Because the population of smart cities is expected to increase at an unprecedented rate over the coming years, there will be a pressing need to make significant investments in the modernization of the city's mobility and transportation infrastructure to make it easier for people to travel both within and between cities. Intelligent transportation systems, also renowned as ITS, resolve as well as provide feasible solutions to logistic challenges. Smart cities are making significant investments in systems that facilitate more robust and flexible transportation and logistics infrastructures, such as the ITS, which also incorporates many other subsystems. All these logistic systems must be secured to preserve the privacy of personal information moving through them to proficiently empower the functionality that ITS offers.

For the satisfaction of citizens, ITS systems allow smart mobility and logistics technologies by maximizing detecting possibilities, evaluating capabilities, managing capacities, and connecting strategies facilitated by the Internet of Things (IoT), Big Data, and Information and Communication Technology (ICT) paradigms [10][11].

Smart automobiles, public transit, many Internets of Things (IoT) devices like smartphones, and numerous controllers like traffic signals, smart traffic signs, and spot sensor actuators; all play a role in making feasible the mobility and transportation options available in smart cities. The Internet of Things (IoT), Big Data, and the Information and Communication Technology (ICT) paradigms empower a variety of technologies that are integral to ITS; including sensor technologies that promote situational awareness, data-driven decision-making, and rapid response.

Computational technologies like encrypted computing, fog nodes, and virtualization improve the ITS services' adaptability, accessibility, dependability, and performance. Analytical technologies in smart mobility technology help guarantee a secure, prioritized system operational environment to enable optimal commute routes based on potential traffics.

Citizens play a significant part in adopting ITS in smart cities. The evolution of ITS services has enabled the process of communicating and interacting with citizens effectively to better meet their needs by using a variety of Internet of Things (IoT) devices. IoT devices in ITS are either owned by citizens or made available to them via deployed kiosks and computers. Because of this, there is a significant number of security risks associated with ITS, all of which must be effectively handled and managed so as not to exacerbate individuals' privacy worries.

The widespread use of Internet of Things devices in intelligent transportation systems (ITS) raises several security concerns related to IoT devices. This is because fundamental data privacy and protection standards are not implemented in many IoT devices, despite the reality that these IoT devices are used in facilitating services provided by ITS [55][56]. Security flaws in ITS sensors and wireless communication technologies cannot be disregarded or dismissed, particularly when they have the potential to affect personally identifiable information (PII) via disruptions in network protocol.

A reevaluation of priorities is needed in smart cities regarding citizens' information when utilizing ITS services since disclosing customers' location information in the ITS infrastructure might be interrupted and rerouted because of cybersecurity weaknesses. Research suggests adopting encryption and authentication mechanisms for smart car security in the controller area network (CAN) [55][57] to ensure security and privacy in multiple applications layers [10].

To ensure that only authorized parties have access to the vehicle's on-board diagnostics (OBD-II) port and, from there, the ECUs and CAN bus, it is crucial to implement eavesdropping [58] and faked packets [59] protection solutions and to secure the car physically [60]. Similar difficulties and assaults relative to denial of service, Sybil [61], and replay attacks are present in wireless network technologies, which may also be found in VANETs. These security concerns can be faced with both types of networks.

To preserve the users' privacy, the privacy remedies in ITS include employing pseudonyms to deliver the services, making the user fictional and even anonymous, and guaranteeing that non-repudiation measures are in place in a way that does not adversely influence the supplied service [10][62][63][64].

To reduce privacy risks, the 3D Privacy basis suggests doing thorough assessments of smart city applications, systems, and procedures related to smart mobility and commuting technologies. This includes determining what data is being acquired and how it may be preserved. Smart mobility and commuting technology in the context of data privacy in smart cities are classified in operational space 1 of the 3D privacy basis, which indicates a significant data privacy risk region that calls for the implementation of statutory provisions in information gathering and solutions for tackling security concerns [54].

Table 1 below provides an evaluation of several prominent security-induced data privacy concerns, along with examples from published literature relevant to keen mobility and commuting technologies in smart cities.

Risk Examples	Security Issues	Privacy Concerns	Feasible Remedy
Spoofing in sensing systems	Active Secure IoT Sensing attack	Authentication Identification	Pseudonym Attribute-based Credentials Message Authentication Codes
Race Condition Timing Attacks	Active Secure ICT Computing attack	Authentication Identification	Public-key Cryptography Symmetric and Asymmetric Key Cryptography
Sybil Attacks on Communication Man in the middle Attacks Eavesdropping	Active secure ICT communication network issues Passive secure ICT communication network issues	Identification Confidentiality Authentication	Attribute-based Credentials Location cloaking Homomorphic Encryption Challenge-Response protocol Steganography
Model Identification attacks Data Intoxication attacks	Active Secure Big Data Machine learning and Artificial Intelligence Issues	Confidentiality Authentication	Signature-based Authentication
Data Intoxication attacks	Active Secure Big Data Analytics	Authentication	Digital signatures Challenge-Response protocol
Parametric/Dynamic Inference attacks	Passive secure Controllers Issues	Confidentiality	Signature-based Authentication Message Authentication codes

Table 2: Privacy Risks and Concerns in Smart Mobility

3.2.1.2. Energy in smart city

If efficiency and optimization are to be guaranteed in smart cities, then smart energy technology must serve as their backbone. Because of the expanding population in smart cities, careful attention must be given to the demand for energy and the production of energy to optimally fulfill the demands of people. In addition, particular attention must be allocated to energy production avenues to assist in the long-term energy demands, since the trend of increasing energy demand is expected to continue.

The technology behind smart energy is at the heart of practically every element of a smart city, including automobiles, sensors, Internet of Things devices, digital traffic signs, toll booths, routers, terminals, and kiosks, amongst other things. To function properly, these elements need electricity for activation and operation, therefore smart cities cannot exist unless they have access to reliable and efficient sources of energy that can satisfy the demands of their residents.

IoT, Big Data, and ICT paradigms play a significant part in achieving smart energy technologies in smart cities. This is accomplished by obtaining information on energy production, consumption, distribution, storage, and waste; evaluating the relevant energy obtained data, and taking informed choices that effectively drive the entire smart energy information system in fulfilling the energy requirements of cities and their residents.

Smart energy relies on cutting-edge technological applications, effective energy transmission, sustainable consumption patterns, and a spotless environment to boost the living standards of individuals without negatively impacting the planet [66][67].

Strategies that meet the energy demands in smart cities include the adoption of renewable energy sources (RES) to produce electricity for many other platforms, systems, and processes in smart cities, which is one example of how smart cities are investing in programs that allow a more reliable and efficient smart energy grid that handles and delivers effective sustainable solutions to the energy requirements of smart cities [68].

While there have been significant investments in RES to deliver enough electricity to fulfill the power needs of smart cities, they have not yet begun to tackle the data privacy and security considerations that total smart energy technology creates. Numerous security-related problems are acquired from the Internet of Things (IoT), the Big Data, and the Information and Communication Technology (ICT) frameworks. Therefore, the 3D privacy basis suggests resolving the data privacy concerns of the technology solutions and their constituents before deploying them in smart cities, by enacting necessary rules that minimize citizens' data privacy worries.

When it comes to monitoring the distribution of energy inside smart cities to families and individuals, there are many data privacy and safety issues because of the ongoing surveillance and measurement of the amount of energy that is spent.

Energy usage is often proportional to the number of people living in a home, therefore there are certain data privacy concerns when this data is made public. Therefore, linking energy usage with periods of the day and connecting it against the presence of people in the residence becomes quite concerning.

This is particularly the case when the information related to energy usage is directly linked with the proprietor or tenant of the house in the smart energy network. Privacy problems arise when IoT, Big Data, and ICT paradigms are used to facilitate services, since individuals may desire a certain source of energy from RES, which may need to be produced off-grid with the extra energy going back to the electric grid. Energy data about which homes contribute how much electricity to the electric grid can also provide a lot of insights.

Since numerous distributed energy resources (DERs) are being built and connected to the grid, there is a greater risk of breaches and cyber threats due to the increased sharing of private information across the network's energy suppliers [69]. The 3D Privacy basis proposes that smart energy solutions, platforms, and operations in smart cities be correctly evaluated to manage and resolve privacy propensities that apply to what personal data is being acquired from homes and how to manage it to guarantee that data privacy issues are alleviated wherever feasible even via regulation.

Table 2 below provides an overview of several prevalent security-induced privacy concerns, along with examples from relevant literature that apply to smart energy technologies in smart cities. These highlighted privacy problems could avoid if the IoT, Big Data, and ICT frameworks that enable them had been painstakingly evaluated and controlled before their deployment in smart cities to prevent the excessive gathering of personally identifiable data.

Risk Examples	Security Issues	Privacy Concerns	Possible Remedy
Power theft Data manipulation Meter controlled by attackers.	Smart meters and power theft attacks	Authentication Authorization	Anonymization Pseudonym Attribute-based Credentials Message Authentication Codes Stealth Operation
US power system attack Spy grid penetration Attacker device control	Active cyber-attacks and terrorism	Authentication Authorization Confidentiality	Public-key Infrastructure Dynamic Encryption Code obfuscation Homomorphic Encryption Meter-based anti-viruses Usage loggers and SM rootkits.
Systems data exposure Lack of self-regulation Lack of reconfiguration	Active operational issues	Authentication Confidentiality	Quality of Service (QoS) routing Pre-programmed self-healing action Smart Grid communication program
Model Identification attacks Data Intoxication attacks	Active Secure Big Data Machine learning and Artificial Intelligence Issues	Confidentiality Authentication	Logical Interface Analysis Real-Time System Monitoring Power system model analysis Computer memory tagging
Data Intoxication attacks	Big Data Analytics Attacks	Authentication Authorization	Incremental Hash Function
Advanced metering infrastructure attacks Pricing attacks data penetration and record attacks	Active digital fraud attacks	Confidentiality	Signature-based Authentication Code obfuscation

Table 3: Privacy Risks and Concerns in Smart Energy

3.2.1.3. Health in smart city

The implementation of smart health informatics in smart cities is a major factor that allows the deployment of a wide range of smart health applications and technologies which enhance citizens' quality of life and improve their standard of living. The expanding population of people living in smart cities necessitates a careful assessment of their health status, both in the short term and in the long term, as they go through and embrace many alterations that occur in smart cities because of tech innovations, services, and processes that they engage with frequently to fully benefit from residing in smart cities.

There is a plethora of health-related Internet of Things devices, applications, and systems that are found in many smart cities. These smart cities make use of Big Data and ICT infrastructures to provide a variety of services for residents.

Because the healthcare and well-being of individuals are of fundamental importance if smart cities are to withstand the challenge of time and solve the rising worries of individuals moving to them, intelligent health technologies must be at the forefront of the existence of all smart cities.

As the COVID-19 epidemic has shown, there are no advantages that are so enticing to overlook smart health and treatment technologies in smart cities. In smart cities, there are numerous smart medical IoT devices, including certain medical fitness trackers, care detectors, smartphone applications, smart glasses, health monitors and medical wristbands, electrocardiograms, blood glucose checkers, EMGs, blood pressure monitors, heart rate monitors, gyro, motion sensors, and other accelerometers, that offer various inherited security problems for residents and produce certain security induced privacy concerns.

All these devices deal with personally identifiable information, and since personal information is transmitted around between systems and devices with varying degrees of data protection, it is vulnerable to hacking and breaches. The Internet of Things (IoT), Big Data, and Information and Communication Technology (ICT) paradigms are crucial to achieving state-of-the-art smart medical technologies in smart cities, as they help to acquire important health information and facilitate the creation of healthcare systems and pathways that react to the immediate healthcare requirements of residents, from nursing babies' temperatures to monitoring an old people's vital signs [70][71].

There are numerous benefits for smart health applications in practically every area of human development. Data collection in smart health applications when combined with appropriate data analysis and decision-making can generate more opportunities to better the health of citizens.

Smart health solutions that improve residents' quality of life and provide residents with channels to stay in touch with their health condition at any time using real-time apps must be made available in all privacy-conscious smart cities. Developments and investments in remedy projects like health embedded systems, pattern recognition, machine learning, and cloud computing address certain individual health problems among residents as smart cities continue to fund and support initiatives in dependable smart health systems that allow the robust and reliable smart medical network to give an effective solution to the long and short-term health requirements of inhabitants [58][71].

The increased use of health sensors to gather individual data and information raises concerns about the security of internet-connected devices, which might be exploited by those with nefarious motives. The identification, authentication, and association of a device with a person's personal information are essential for proper health monitoring and evaluation.

Given the persistence of several inherent security-related problems concerning IoT, Big Data, and ICT paradigms, the 3D privacy basis suggests in the case of healthcare systems that data privacy implications with smart health technologies and their elements be addressed before their deployment in smart cities through effective legislation that diminishes citizens' data privacy worries to promote the emergence of privacy-aware smart cities.

There are several potential points of failure in the acquisition of personal data that is associated with smart health devices, including the connection technologies employed, the patient care systems accessed, and the end-user interaction inquiries, such as adding or updating information [70]. Most smart health systems associated with a single user require some type of authentication and authorization for information collection or retrieval which raises ethical challenges in smart cities.

As a result, users' health data is sent over interconnection protocols including area network, NFC, Bluetooth low energy, Zigbee, and satellites, utilizing a wireless device where pseudonyms [59] and anonymization [54] paired with encryption [65] are employed to safeguard personal information.

Public health is at serious risk when considering the potential of harmful actions like giving incorrect medications to a patient due to a malicious attack compromising the patient's prescription information.

Additionally, there are privacy concerns when thinking about on-body sensing devices that continuously gather and transfer patient data utilizing connection protocols that may be broken in and provide access to health information tied to the on-body sensing device [70]. Insecure internet or connection protocols involving data traffic volumes [70] pose a threat to the privacy and integrity of the data collected by many connected devices utilized and associated with other IoT devices through communication media that enables instant message (short message services), NFC (near field communication), Wi-Fi, and social networking.

It is recommended by the 3D Privacy basis that smart digital health systems in smart cities be adequately assessed to better manage data privacy threats. This is because the security flaws involved in safeguarding a smart medical system are ubiquitous, and the smart health system contains essential personally identifiable information that may be very detrimental if it is accessed for malevolent purposes [66]. Because of the possibility to collect more private data in the delivery of health services to facilitate timely and effective patient treatments, the 3D Privacy basis places smart health technology in operational space 2 which indicates a high data privacy risk zone [54].

Table 4 below provides an overview of some pervasive security-generated privacy vulnerabilities along with instances from literature relevant to smart health technology in intelligent cities. These difficulties could be avoided if the IoT, Big Data, and ICT frameworks that enable these applications were painstakingly evaluated and controlled to prevent the excessive gathering of personally identifiable data before their implementation in smart cities.

Risk Examples	Security Issues	Privacy Concerns	Feasible Remedy
Denial of service with the right credentials attack Data Intoxication False diagnostics Treatment attack	Active Location based issues	Authentication Authorization	Pseudonym Attribute-based Credentials Message Authentication Codes
Fabricated node identity attacks	Secure ICT Fog and cloud Computing attack	Authentication, Authorization	Cryptography Tamper-proofing via Blockchain Data dissemination via FoG M2M messaging with rule-based beacon Attribute-based access control
Jamming communication channels Sybil Attacks in communication Replay attack Eavesdropping Blind letter attack Routing attack	Secure Communication network issues	Authorization Authentication Confidentiality	Attribute-based Credentials Location cloaking Homomorphic Encryption Challenge-Response protocol Steganography
Fake emergency call attacks Data Intoxication attacks	Big Data Machine learning and Artificial Intelligence Issues	Confidentiality Authentication	Signature-based Authentication
Insider and outsider attack Data Intoxication attacks	Big Data Analytics issues	Authentication	Digital signatures Challenge-Response protocol
Dynamic Inference attacks	Passive secure Controllers Issues	Confidentiality	Signature-based Authentication Access-based authentication Message Authentication codes

Table 4: Privacy Risks and Concerns in Smart Health

3.2.1.4. Governance in smart city

When it comes to achieving the aims of smart cities and assuring the pleasure of their residents, smart governance technology is the overarching concept that includes other smart technologies. To city administrators, this appears more important than any other smart technology since it demonstrates to residents that their money is well spent on systems that would help them out in the long run.

As smart cities continue to attract more residents, they will need to carefully consider how their government, residents, and stakeholders can best work together to realize the full potential of their smart communities [8]. The Internet of Things (IoT), Big Data, and Information and Communication Technology (ICT) are all part of smart governance technologies, which improve the legal government decision-making process in smart cities so that their government and residents interact together more effectively to facilitate the adaptation to new systems and technology.

It is possible to define smart governance in the context of smart cities as the ability of the government of a smart city to make use of the intelligent and adaptable resources at its disposal to facilitate better decision-making about its systems and procedures for the benefit of its residents, to ensure greater effectiveness and a higher quality of life in the short and long term [10].

The viability of smart cities depends on the quality of life and wellness of their residents which renders effective smart governance crucial in smart cities. Data governance, citizens, ecosystems, and technologies allow the smart governance ecosystem to incorporate ICT-based technologies like social media to solve many governance issues pertaining to transparency, openness, democracy, citizen involvement, and information exchange.

There is no denying that the Internet of Things (IoT), Big Data, and Information and Communication Technologies (ICT) frameworks are present in smart governance technology. They increase the possibility of security flaws, which accentuate data privacy problems that must be resolved in smart cities if they are to evolve into privacy-aware smart cities.

Since data and information flow through the smart governance ecosystem can be compromised, there is a huge need to properly comprehend and differentiate the flow of personal and impersonal data. This is critical because there is a larger likelihood of overlap while providing services, where it may be difficult to separate, for instance, an individual's viewpoint from what they stand for and with whom they identify [10][11]. Technology plays an essential part in this area because it expands how residents may provide feedback and communicate with their government officials, which is a prerequisite for the improvement of urban services.

Electronic government (e-government) and electronic governance (e-governance) fall into the highest data privacy zone of the 3D privacy basis, and they help solve the government’s demands in smart cities in many ways as cities engage in systems that allow more accessible and adaptable smart governance technologies that tackle and deliver optimum governing responses to the requirements of residents in the short and long term.

Inherent security concerns plague both e-government and e-governance smart methods due to the Internet of Things (IoT), Big Data, and Information and Communication

Technology (ICT) frameworks involved in realizing interaction and connection between the smart cities administration and their residents via citizen involvement expressing citizens' perspectives in smart cities [11][53][54].

The 3D privacy basis advocates for analyzing the privacy risks posed by governance technologies, applications, and their related components before implementing them in privacy-aware smart cities via the implementation of appropriate rules. When the demand for citizen engagement is addressed anonymously and without sufficient validation that the people responding are indeed residents of the specific smart city in question and not just tourists, then there are privacy problems that arise [72].

Sensitive personal information may be transmitted and compromised throughout the data collection process used to validate a citizen's residency in a smart city and make suggestions to the local authority via custom e-government applications. Monitoring people's feelings in smart cities through social media raises comparable data privacy issues [72]. Solutions to issues of democracy, socioeconomic inequity, and justice all involve some type of identification and verification, which puts people’s personal information in jeopardy and provide an avenue to compromise people’s right to privacy [72].

The 3D Privacy basis supports the evaluation of smart city technologies considering smart governance technology's control of privacy vulnerabilities related to what data is being acquired from residents and how to handle personal data to guarantee data privacy issues diminish among citizens whenever feasible even via regulations [54]. According to the 3D privacy basis, smart city government and governance fall into operational spaces 3 and 4, respectively [54].

These operational spaces are associated with the greatest privacy threats and necessitate the adoption of data collection standards to provide an avenue to address data security and privacy problems proactively to avoid breaches of more sensitive information. It is essential to determine how the privacy of residents in smart cities might be compromised by the smart governance applications, systems, and procedures that are put into place to allow technological solutions that profit citizens without interfering with their privacy. Regulations must be put in place to make sure that both the already deployed technologies and those that will be deployed in the future do not continue to violate the privacy of individuals or put them at risk of criminal prosecution.

Table 5 below presents an overview of some substantial security-induced privacy concerns, along with instances from literature related to smart governance technologies in smart cities, which can be avoided with careful assessment and regulation of IoT, Big Data, and ICT frameworks to prevent the excessive gathering of personally identifiable data before their implementation in smart cities.

Risk Examples	Security Issues	Privacy Concerns	Feasible Remedy
Denial of service attack remote exploitation sensor-controlled failure Data Intoxication anonymity attacks	IoT security issues	Authentication Authorization	Pseudonym Anonymization Attribute-based Credentials Message Authentication approach
Data leakage Malicious insider attack Insecure API Malware injection attacks Digital disenfranchisement	Secure ICT Fog and cloud Computing attack	Authentication Authorization	Cryptography Blockchain Encryption
Impersonation attacks Insecure protocol Third parties' attacks Lasting trust issues	Secure Communication and social media network issues	Authorization Authentication Confidentiality	Attribute-based Credentials Location cloaking Homomorphic Encryption Challenge-Response protocol Steganography
Data Intoxication attacks Bias algorithms Profiling location-based issues	Big Data Machine learning and Artificial Intelligence algorithms Issues	Confidentiality Authentication	Signature-based Authentication
Insider and outsider attack Sentiment misinterpretation Opinions versus facts dilemma	Big Data Analytics biasing issues	Authentication	Digital signatures

Table 5: Privacy Risks and Concerns in Smart Governance

As IoT, Big Data, and ICT paradigms continue to proliferate tech innovations without generating more security risks associated with the users of these technologies, then many privacy-aware smart cities may begin to form. This will ensure that there are no data personal protection gaps that must be closed to keep smart cities functioning smoothly. There is a clear prevalence of authentication, identity, authorization, and data privacy problems in almost all the deployed smart cities technologies that must be addressed through various comparable solutions described in the different tables. To ensure that residents' privacy is protected throughout the lifecycle of a service and beyond, smart cities must implement the 3D privacy basis recommendations.

In doing so, people’s privacy will be safeguarded before they ever use the tech-enabled services, which will greatly lessen the likelihood of data privacy compromission in the first place. Thus, more privacy-aware smart cities may be realized by completely resolving security concerns related to IoT, Big Data, and ICT paradigms in smart cities through the implementation of policies that support the protection of people’s data privacy.

3.3. Smart Multimedia Privacy Concerns

The change in a great number of cities all over the world has been made possible by their adoption of a wide variety of cutting-edge multimedia technologies, which are currently accessible to them and serve to define their goals in a variety of different ways. It is worth noting that advanced multimedia systems and technologies play a crucial role in facilitating smart city projects. Therefore, intelligent multimedia technologies and systems need to undergo a comprehensive evaluation considering the numerous security risks that are described in the published research to provide an adequate response to the numerous privacy concerns held by residents of smart cities.

When considering the intricacy of the privacy concerns surrounding smart multimedia technologies and systems in smart cities, it is important to remember that privacy is, first and foremost, a problem that affects each person living in a smart city. Despite this, smart cities must find a way to work together to develop a solution that considers the privacy concerns of the whole city as well as those of its residents.

This chapter presents a unique strategy for resolving the citizens' data privacy issues in smart multimedia technology. The strategy involves collecting data and processing it at the edge with the available artificial intelligence and machine learning technologies to analyze, personalize, and classify the multimedia content at the point of data collection. These concerns relate to smart multimedia technologies and systems that are engaged with the text, audio, image, and video data processing.

3.3.1. Data Privacy Solution Context

From auditory, speech, and voice recognition to picture and object identification and even face recognition and human-computer interaction technologies, the existence of smart interactive media technologies and systems is evident and pervasive in several of the advancements that enable smart cities. Smart multimedia technologies have become an integral part of practically all the activities and initiatives that make it possible to turn a city into a smart city [65][73][74].

This is especially true in terms of the audio, voice, picture, and intelligent video surveillance use cases that these technologies enable. There are significant security concerns for multiple multimedia systems used in smart cities as well as the technologies that enable them. Smart multimedia devices and systems continue to be a primary entry point for cyberattacks and hazards in smart cities. Numerous security vulnerabilities connected with intelligent multimedia innovations are explored in this chapter, although only at a high level.

This chapter primarily focuses on three kinds of smart multimedia systems namely audio, sound, and voice recognition [74], picture and object recognition [65][75], and real-time video processing detection and analysis [56] that allow many crucial monitoring systems that are highly dependent on these tech innovations for their operation. These systems' primary flaw is that they enable open channels that facilitate the gathering of individual information via a single data stream with varying degrees of data privacy implications depending on the significance of the collected data, some of which may carry information relating to confidentiality whereas others may not.

The audio collected by an IoT device, such as a microphone, is the sum of the audio frequencies captured from various noise sources in the immediate area of the instrument. If many sounds, such as a gunshot [54] occur in the vicinity, a citizen's phone discussion, a sound of an approaching vehicle, or the rush of traffic, were recorded at the same time, the resulting audio would contain a contributing element of each of these sound components. While many people in smart cities may not want their voices or other audible signals recorded, there are already many vocal data sets acquired from them [54][56] that have been recorded in a variety of settings without their knowledge or agreement.

Many object recognition systems and technologies operate under a similar premise, wherein a captured image of a possible target captures the target itself, in addition to other objects surrounding the target and possibly even people who did not give their media rights to be included in the captured picture. As a result, data acquired by IoT devices to power various smart multimedia platforms can be composed of multiple constituent pieces with varying degrees of privacy leading to many smart multimedia platforms raising significant privacy problems.

Recently developed machine learning and artificial intelligence techniques have opened promising avenues for dissecting a multimedia data stream into its constituent parts, each of which may be assigned a different level of data privacy protection. The overall level of privacy protection for the video stream can then be set to match the highest level of data privacy protection for the most sensitive portion of the video stream. Because of this, the capturing, storing, and processing of the data components deemed to contain private information may be done with a greater degree of consideration regarding its analysis, usage, and storage.

To properly analyze the privacy concerns involving these smart multimedia technologies and innovations, it is crucial to discover and propose strategies that reduce and diminish citizens' privacy worries as individuals use and accept more intelligent multimedia services, technologies, and systems. As a result, smart cities must solve the problem of acquired multimedia data, which can be a continuous accumulation of numerous separate multimedia content such as video feeds collected with sound, to adequately meet residents' privacy concerns inside smart cities.

When it comes to data privacy in smart cities, everyone's worries are different. If smart cities are going to work together to solve a problem for their residents, they need a system in place that can link captured information to a person rather than a group of people, because individuals within a group may have different ideas about what counts as personally identifiable information. As a result, this chapter presents a method for characterizing acquired information with the progress of artificial intelligence through machine learning techniques and associating it with a particular individual rather than a group of people to enable a closer evaluation of data privacy concerns and privacy levels relevant to intelligent multimedia platforms and innovations inside smart cities.

3.3.2. Smart Multimedia Systems

This chapter examines privacy issues with image and vision systems, audio and voice systems, and biometric systems. When it comes to privacy concerns regarding the safety of intelligent multimedia systems, the fact that they have vulnerabilities at both the physical and the digital levels cannot be overlooked. Intelligent multimedia-connected devices that gather people's data must have robust physical protection in terms of who might reach or manage them as their underlying technology security.

Many security-related concerns in smart cities arise from the existence of these two levels of security. These levels of security must be discussed and addressed before residents embrace the privacy-conscious concept of smart cities and its promise to eliminate the risks of security-induced privacy-related concerns [76]. Many privacy issues occur from the widespread deployment of intelligent multimedia IoT gadgets in intelligent cities, where hardly or no control is exercised over the specific portion of the data they collect. For instance, audio recording devices [66][77] record all the sound and audio wave signals from their immediate surroundings regardless of geographic location, even though some citizens may not give permission to be recorded in such settings.

Similarly, in smart cities, residents [66][76] may not realize they are being filmed on camera and so they may not provide their informed agreement for their picture or video to be gathered.

Therefore, to create privacy-aware smart cities, it is important for these communities to acknowledge and appropriately deal with this possible avenue of security-induced privacy issues. Face detection [65], audio recognition [74], motion detection [55], temperature sensing [66][77], and many more brilliant multimedia applications [76] are just a few examples of the smart multimedia systems and technologies being empowered currently in smart cities thanks to the emergence of smart multimedia connected devices [68].

Privacy concerns emerge because of multimedia systems' broad data gathering points, which may collect data from many different people simultaneously in one massive data stream. As a result, they must be examinations of each component of the system to assess the general privacy level of the recorded data stream. If hackers were to get access to and take control of the IoT device at the point where the data is collected, then the technical security dimension poses an even higher risk to individuals' right to privacy.

As a result, the information of several citizens may be put at risk. The privacy and security concerns that arise from processing data collected by IoT devices close to their place of data collection have prompted several suggested solutions [68], but these solutions do not go to the heart of the issue, which is determining whether the technology is ready for implementation in smart cities.

The possibility of using smart multimedia Internet of Things devices in smart cities continues to be one of the largest assets and facilitators of opportunities in smart cities [68]. Prospective solutions for smart cities will significantly rely on the creation and integration of multiple intelligent multimedia Internet of Things devices that can assist in the characterization of various input signal sources.

3.3.3. Method Significance

Today's sophisticated multimedia capabilities provide several advantages that may be used to address and mitigate individuals' data privacy worries. To differentiate between two people, developments in sound, vocal, and speech technologies have made it possible to identify and recognize people's voices using all the distinguishing qualities necessary. This same technical development may be utilized to assign varying degrees of privacy to various aspects of captured audio signals and to dampen the tones and frequencies that carry the most sensitive personal information using digital signal processing filters [68], as depicted in figure 6 below.

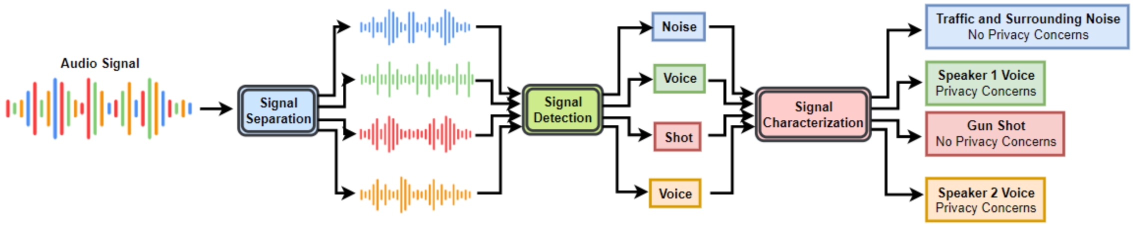

Audio Signal
Signal Separation
Signal Detection
Noise
Voice
Shot
Voice
Signal Characterization
Traffic and Surrounding Noise No Privacy Concerns
Speaker 1 Voice Privacy Concerns
Gun Shot No Privacy Concerns
Speaker 2 Voice Privacy Concerns

Figure 6: Characterization and Classification of Audio Signals for Privacy Purposes.

This method may also be used to evaluate picture and video recognition and identification systems, as each image is composed of many individual pixels, and the privacy degrees of every given pixel or set of pixels will vary depending on the importance of the content they contain. As shown in figure 7 below, a taken picture may be broken down into portions with varying degrees of privacy responsiveness depending on the number of people whose identities are revealed by pixels inside the picture.

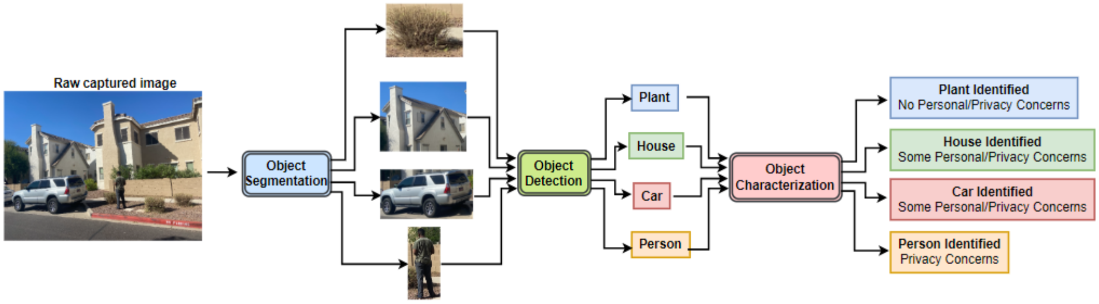


Figure 7: Characterization and Classification of an Image Frame Data to Protect Privacy.

This strategy will inspire and stimulate a new field of scientific studies about data privacy in tech applications, while also doing so by using the existing sophisticated methods and technologies in artificial intelligence and machine learning to characterize segments of multimedia content based on the significant privacy thresholds as described by the 3D privacy basis [54].

Facial recognition algorithms need to employ this method since various faces identified in video data streams may be segmented into multiple mini-data feeds for each face recognized in the stream. In that same way, the non-targeted individuals in the stream can be removed or blurred in the data feed to preserve them for data privacy purposes. The goal of such granular categorization and customization of multimedia content feeds is to assign different degrees of confidentiality to the various data stream components in accordance with the information they contain and expose.

It is crucial that smart cities prevent collecting huge datasets that may not be necessary and are not utilized to implement valuable systems or technologies. To prevent gathering unnecessary data while profiling people in smart cities, it is crucial to develop more effective methods of extracting and analyzing smart multimedia content.

The 3D privacy basis [54] advises monitoring any type of smart interactive multimedia, service, platform, and activity through the eyes of the average citizen to ascertain how acquired personal information may be kept private over time and not connected to other information that has the potential to characterize or identify an individual.

Therefore, it is of the utmost importance to grasp how smart multimedia operations are conducted and supported in smart cities, particularly those that are engaged in the gathering of personally identifiable information. This may be accomplished by establishing and analyzing the smart multimedia IoT gadgets or systems that are connected, the multimedia content that is being collected and stored, as well as the overall data transmission and technological data transformation pathways that enable decision-making. This is because data may transcend across multiple various types of systems with different data security protection.

3.3.4. Method Application

Several obstacles must be overcome to enable the incorporation of such mechanisms with the already deployed legacy applications to implement them on a large scale and inside smart cities. There are numerous factors to consider before realistically deploying AI-driven data categorization and personalization, but some of the most important ones are cost, computational power, feasibility, and citizen experience.

Because there are so many kinds of data, including text, audio, image, video, biometric, and so on, that need to be taken into consideration, the methodology of classifying and personalizing multimedia data feeds to classify various privacy risks will initially necessitate a substantial amount of financial investment. This is because of the severity of the various types of data that must be accounted for.

It is going to be necessary for smart cities to have a better understanding of how to handle each type of data and determine the types of information that should be retained from each data type [54]. In addition, a sizeable amount of capital is required to cover the expenses involved in locating and modernizing outdated computer systems to enable AI capabilities.

As more kinds of data are generated and as more Internet of Things devices is put into use, the increased expense of maintaining a support tech team to ensure that the systems continue to perform as intended will continue to be a burden for smart cities, both in the short and long term. The expense of establishing this system will be the biggest barrier for tech businesses and smart cities to widely disseminate AI-enabled data categorization and personalization technologies for coping with citizens' private information.

The computing power of IoT devices for data collection is crucial to facilitate the fulfillment of the suggested AI-driven data categorization and personalization with privacy evaluations to better manage citizens' personal information. Before the data can be transported to be preserved in repositories, the Internet of Things devices that are capturing the data must first be updated with sufficient processing power to allow for the data characterization process to be carried out smoothly at the collection point.

Because not all computer chips used in IoT devices can compute, process, and carry out AI data characterization and customization, it will be necessary to upgrade the processors used in many IoT devices for better data characterization during the data acquisition process.

Although computer chips are getting faster and more powerful, this does not necessarily indicate that all the Internet of Things sensors must be upgraded with the most powerful processors available for the job. Considering this, it is crucial to equip the IoT devices used for data gathering in smart cities with processors that offer the appropriate computing prowess required to perform AI data categorization and personalization.

The large number of legacy systems currently in place in smart cities, including databases and applications that rely on them, poses a significant barrier to the rapid and reliable deployment of AI data categorization and personalization.

The fact that all the dependent legacy systems would still anticipate data in the legacy form rather than post-processed data with some contents deleted or some restrictions imposed is a crucial source of worries regarding the viability of AI data categorization and personalization with legacy systems. It is possible that the required network infrastructure may not have the practical capacity to support the integration of older devices, which would be necessary for maintaining strong dependability and security while also optimizing the data management process.

It is of the utmost importance to have a solid understanding of which aspects of the legacy systems can be relevant in the implementation of AI data characterization and customization processes to facilitate the appropriate categorization of data. Because of the vast quantities of advancements that have been made in software and hardware, it is not simple or easily viable to integrate new technologies with legacy products.

Due to the operating costs and delays that occur when processing the data and fulfilling the users' demands, installing the AI data classification and personalization during data collection presents a unique set of challenges that must be overcome to provide a positive user experience.

It is impossible to understate the user experience's significance when considering the possibility that citizens will not tolerate any further delays in getting replies to their requests or in the fulfillment of such requests. Because the data that is often gathered first must be assessed and classified, the user experience will suffer because the data cannot be delivered to the database until after it has triggered the response that users may be waiting for.

Therefore, the addition of an interim step into the workflow for data processing would increase the amount of time required to fulfill the users' requests. This may not be acceptable for certain users, and as a result, they may give up on some applications. This is especially likely to happen when the data collection, categorization, and personalization processes are complex and demand a large amount of computation time. The user experience is a crucial component because it plays a significant part in assisting residents to better navigate through the innovations made possible by smart cities leading to the enhancement of both the general well-being of users and their quality of life.

Since the implementation of AI-driven data characterization and customization in smart cities might provide benefits from assigning privacy degrees to data and developing the required data handling procedures, it is imperative that all the previously described criteria above be properly considered.

3.3.5. Method Inference

It is of the utmost importance to consider how security risks associated with intelligent multimedia systems can spread to other types of technologies and leave gaps that must be filled to prevent further invasions of citizens' right to privacy brought on by their use of intelligent multimedia technologies and services in smart cities.

The strategy that is being offered of classifying and customizing multimedia feeds to categorize distinct privacy consequences would help safeguard and defend citizens' private information long before they gain the benefit of tech multimedia services. This is preferable to avoid permitting multimedia services without adequately resolving privacy problems that may afterward occur.

As intelligent multimedia IoT devices are utilized, Big Data is expanded, and ICT systems and methods used to complete and conduct clever multimedia services are extensively evaluated and categorized, the 3D privacy basis may leverage the suggested methodologies and offer a unique manner of resolving security-driven privacy issues for citizens [54][75]. More privacy-conscious smart cities will rapidly emerge when the 3D privacy basis recommendations for addressing and regulating intelligent multimedia data privacy and security problems throughout all installed multimedia elements, services, and networks in smart cities are implemented.

CHAPTER 4

TECH DATA PRIVACY SURVEY

4.1. Survey Planning and Conduction

A survey was conducted for this research comprising a total of seventy-three (73) questions concerning the interaction of users with tech applications for various interests, purposes, and uses. The survey questions targeted the quantitative and qualitative interaction of users with tech applications for various interests and purposes pertaining to users' propensity to share their data in return for valuable services provided by tech applications. The survey was completed by students, friends, and affiliated members of different student groups of Arizona State University yielding a sample size of 228 participants (n = 228).

The survey aimed to gain a better understanding of citizens' privacy concerns encountered while engaging with technologies through using tech applications and receiving tech services in smart cities. Thus, the participants' experience and opinion on information collected by tech applications was targeted to identify what information they consider private and how they prefer their personal data to be handled in tech applications.

The survey consisted of fourteen questions related to general information about the user pertaining to their social status. It also contained thirty-nine questions pertaining to users' use of tech applications at various intervals and for various reasons. The survey likewise had fifteen questions pertaining to how users share their data; for what motif and in what circumstances they share it. Finally, the survey included five questions related to the user's awareness of the tech application attacks, dangers, and organizations that enable tech applications in digital spaces.

The survey comprised three different types of questions involving single-answer multiple-choice questions, yes or no type questions, and multiple answers multiple choice questions with fill-in-the-blank options. The survey completion duration to answer the 73 questions ranged from 30 to 45 minutes. The users' survey responses were aggregated based on several factors like data types, applications' utilities, users' preferences, time spent on the app, and frequency of interactions, etc.

An email invite to complete an electronic google form of the survey containing the following link (https://docs.google.com/forms/d/e/1FAIpQLSdu0IXOI21igivDKxhSbIMmokQArntXcBtiU4BjrhqzxrgmSw/viewform?usp=sf_link) was sent to the undergrad and grad student body of the Arizona State University. Out of the students and affiliated student club members of Arizona State University that received the survey request, a total of 228 people responded by the survey collection date of August 31, 2022.

4.2. Survey Insights and Discoveries

The survey's data analysis of participants' responses indicated that users interact with tech applications for many reasons and indeed share their personal data in the process. The survey's data analysis showed that there is some personal information that users deem more private and sensitive than others, and they actively avoid sharing this private and sensitive personal information online or in tech applications.

The survey revealed the constant disturbance of users by unwanted tech solicitations via disturbing unknown phone calls and flooding email solicitations. The survey exposed that most users frequently interact with tech applications without clearly understanding all the personal data that is collected from them in the process nor understanding the policies that govern the tech application data collection process.

The survey revealed that most users want to control their personal data and data privacy, and they would appreciate a technological means to facilitate that. The survey also revealed that users have adopted tech applications, and they are willing to share their personal data for services that they need and find valuable especially if there are aware of how their personal data is enabling the services.

The survey likewise revealed that users have embraced tech applications, but they are still very skeptical of their data privacy on the internet. The survey similarly revealed users desire technological means of controlling their data privacy on the internet to distinguish between their more private personal data from the rest.

The following figures showcase ten selected survey responses summary that reveal user sentiments and choices regarding their data experience while using tech applications. More survey summary figures are presented in the appendix section B.

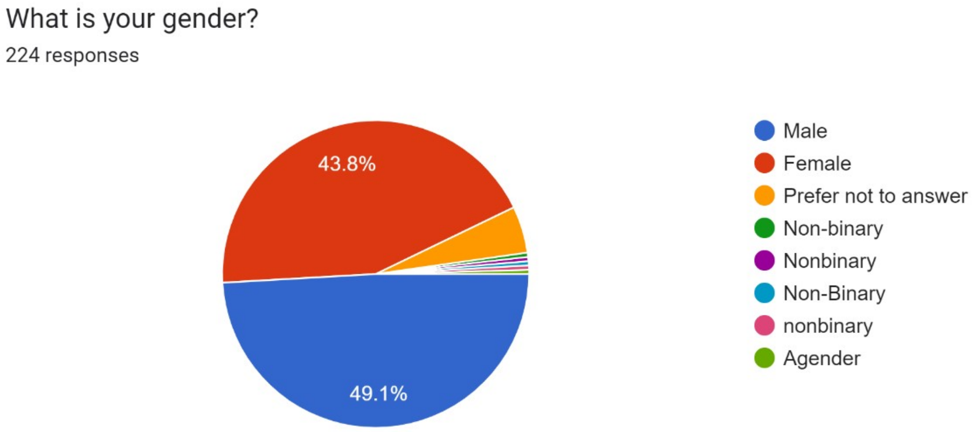


Figure 8: Survey Response Summary of Survey Question 1

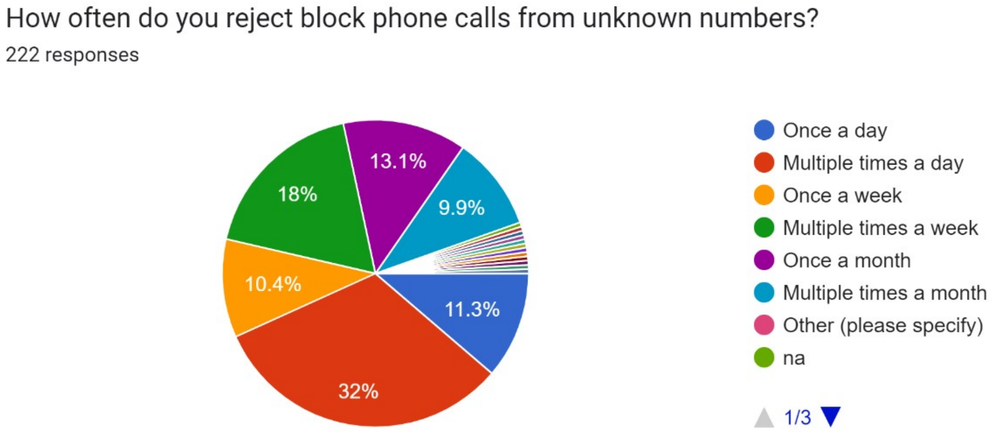


Figure 9: Survey Response Summary of Survey Question 45

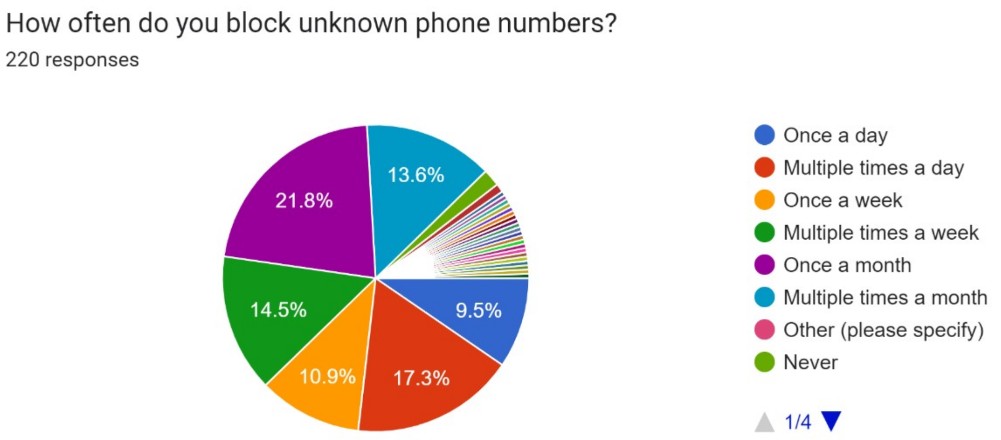


Figure 10: Survey Response Summary of Survey Question 46

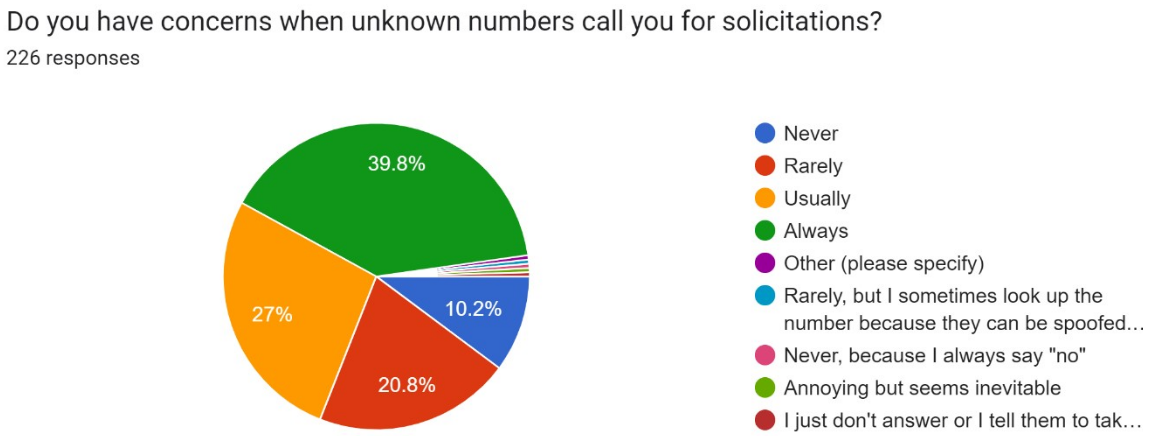
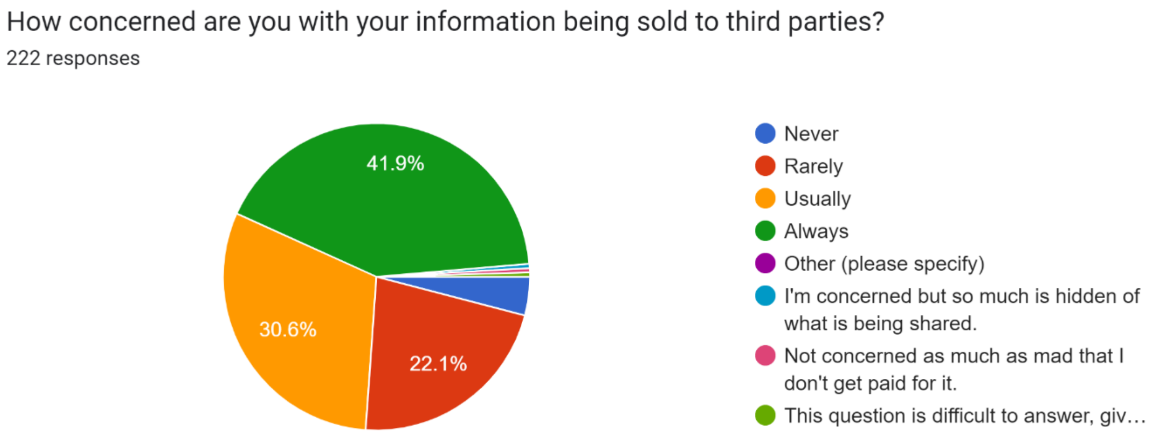


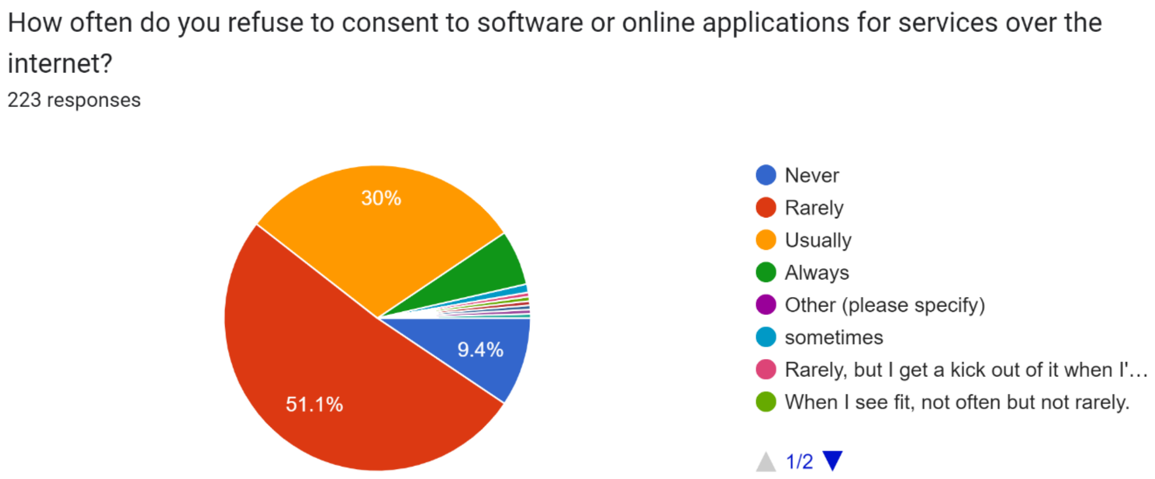
Figure 11: Survey Response Summary of Survey Question 47



How concerned are you with your information being sold to third parties?

222 responses

Figure 12: Survey Response Summary of Survey Question 48



How often do you refuse to consent to software or online applications for services over the internet?

223 responses

Figure 13: Survey Response Summary of Survey Question 69

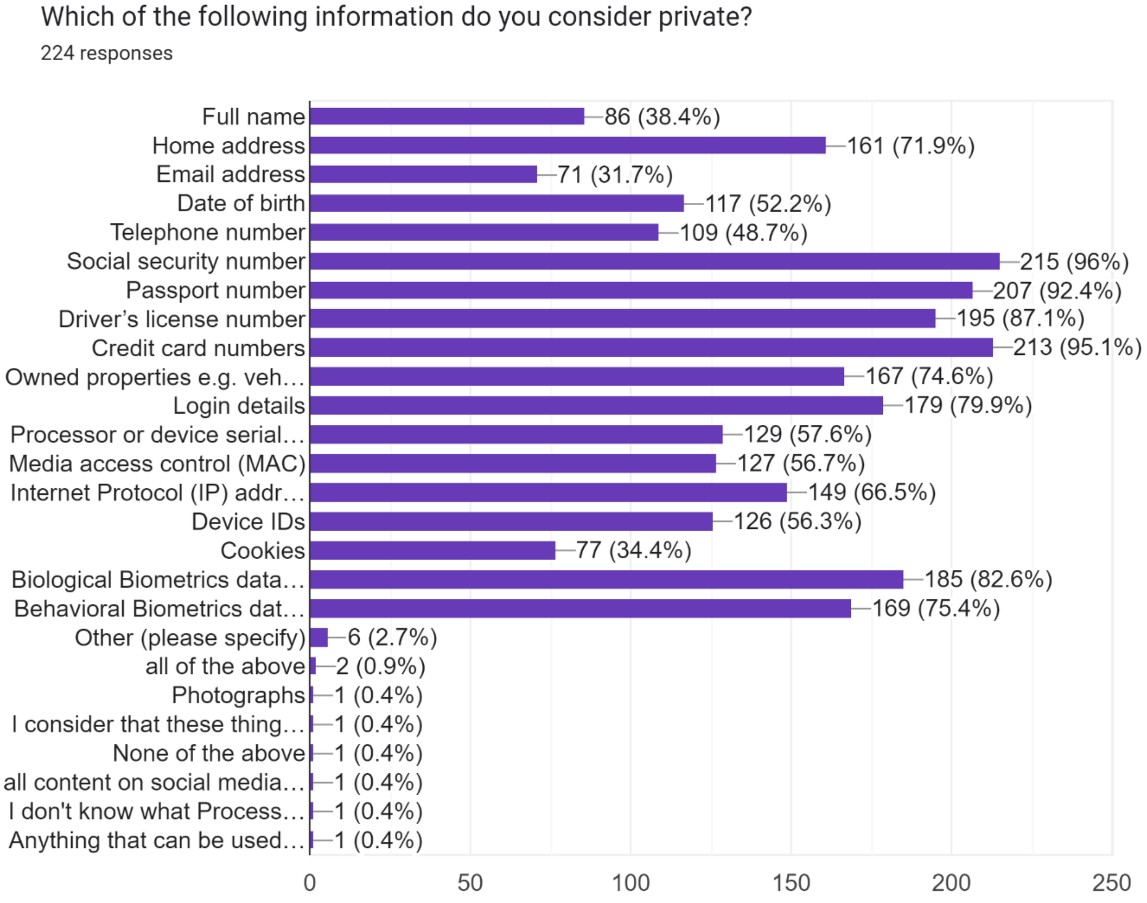


Figure 14: Survey Response Summary of Survey Question 51

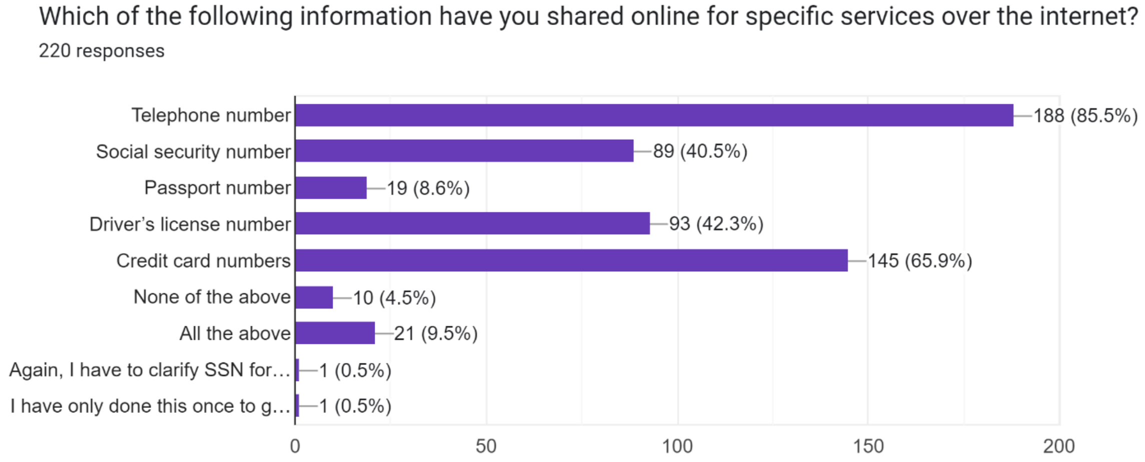
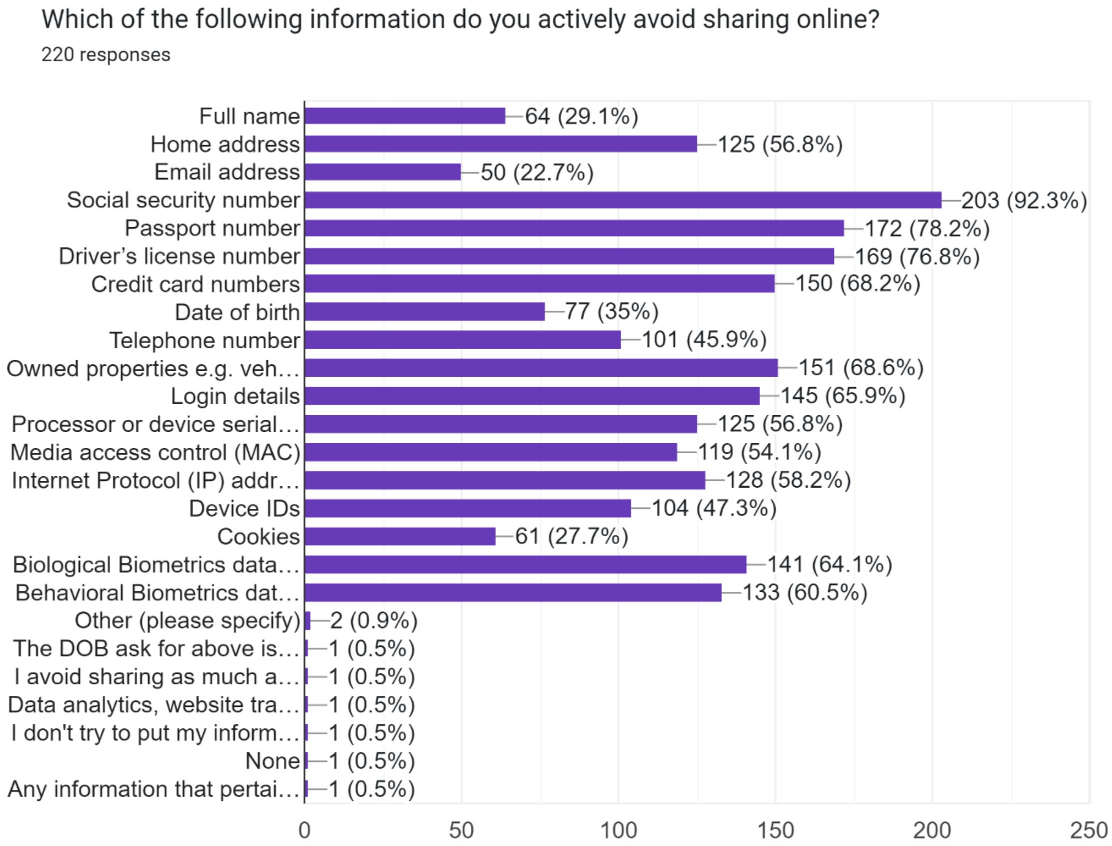


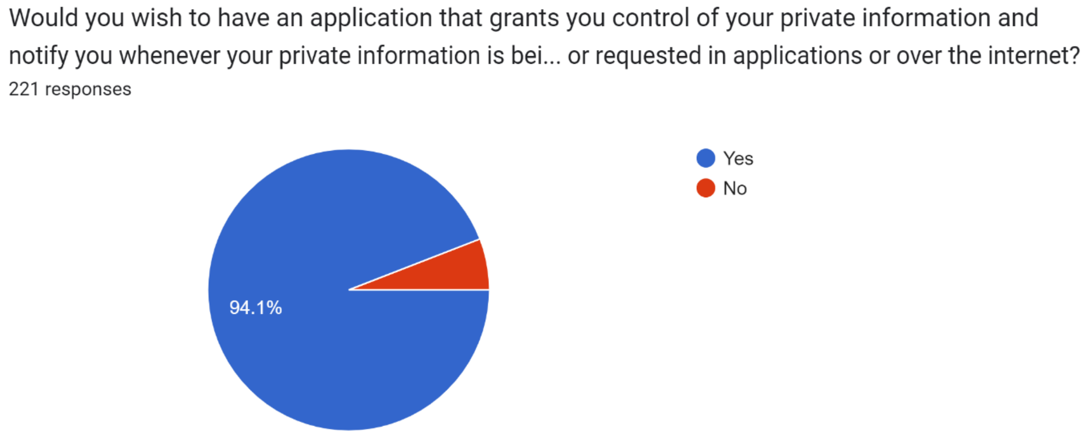
Figure 15: Survey Response Summary of Survey Question 63



Which of the following information do you actively avoid sharing online?

220 responses

Figure 16: Survey Response Summary of Survey Question 66



Would you wish to have an application that grants you control of your private information and notify you whenever your private information is bei... or requested in applications or over the internet?

221 responses

Figure 17: Survey Response Summary of Survey Question 70

CHAPTER 5

PRIVACY CONTROL AND APPLICATIONS

Another way to consider privacy in tech applications is to define it as the right to be disturbed by tech applications or services that one wants to be disturbed by. Thus, the question of user data privacy in smart city tech applications depends predominantly on users themselves as they are the biggest players in facilitating progress in the user's data privacy space. Users must decide when, how, and by what tech applications they want to be disturbed. The way tech applications are built nowadays only strengthens and multiplies the risks for users to receive unwanted emails, solicitations, and annoying calls due to how easily personal data is collected and managed in the tech application data workflow.

It is important to implore technological advancements to help resolve these data privacy issues by giving users the control of their data back to make them the deciders of what personal data to share and when to delete it. User preferences on what tech applications to download and install are based on the value they receive relative to the value of the personal data they are willing to provide.

User data control is key in enabling user data privacy even on the web considering the possibility that affects the data distribution and management of tech applications directly at the point of data collection. It is pressing to enable user data control sooner before it becomes too late and more challenging to control personal data sharing. Thus, since no one can control what others can do with their data, it is paramount to make sure users are aware of available data privacy threats, and the role they can play to minimize or eradicate their data privacy risks.

Similarly, it is important to grant tech application users the ability to control their personal data even after they have shared it so that they can play an active role in owning the responsibility for their data privacy in smart city spaces.

Therefore, how can user data privacy awareness be achieved in tech applications? It is by sensing, surveying, and understanding what constitutes users' personal information, and what tech applications are doing with personal data after they collect it based on the promises and responsibilities outlined in their software service agreements or terms of use. The assessment of data collection and usage within the tech application given the privacy implication of the data that is being collected is critical to ensure users are aware of the privacy implications of using the tech application.

The benefit of real-time flagging and warning notification technologies will help users to be reminded of some privacy implications pertaining to the personal data they are willing to share. For example, when information pertaining to users' credit card, ID, and social security numbers is shared, a tech application can flag or notify the user every time they want to share or post their credit card numbers, ID, and social security numbers of the potential data privacy risks associated with their personal data. In this manner, users will be aware and able to decide whether they are making the right move in providing personal information. Real-time response to potential data privacy issues is a proactive approach to help build and improve user awareness.

It is a great point of collaboration between users and tech application makers to enable users in becoming partners in minimizing the overall tech application data privacy risks. Another solution approach is to enable users to control their data even after they have posted, share, or release their personal information to tech applications. This is crucial, especially considering the security network issues that can arise due to different media of data protection within the security envelope responsible for safe data transfer from one endpoint to another.

There are a lot of glitches in information sharing that can be aggregated and taken advantage of to further extra critical information from network data packets. Users must have a say and control over what data they are willing to share, whether their data is posted in tech applications for their use only, and for how long their data should be used. This is important because most of the time data privacy threats are not in using users' data but in storing their data for a long period while accumulating, generating, and aggregating more personal data.

If personal data was simply used to determine trends and patterns to enable some anticipated value extraction, and then discarded without storing personally identifiable information, then data privacy risks would be minimized. The conflict between the citizen value and the city value comes mostly from the way personal data is treated because the citizens' interest is more immediate as in the here and now while the city's interest is in the future anticipations and prediction.

For example, a citizen or user may need to use a tech application for a service, and once they have received the service, they can be completely done with it and do not have to deal with it anymore. However, the city's view is quite different as it plans to store and use this data to predict in what capacity it can best serve the citizens in identifying where and how to manage and allocate its resources.

Cities are focused on the big picture and scale, but it is important to go to that scale with the user's inputs about what they want and care about, and what tech applications they are willing to enable. Unless aware users give their preferences, it remains a challenge to control what information users post and how to handle it. Thus, developing a data privacy control application architecture and prototype is critical to streamlining how to handle users' data sharing.

A data privacy control application is an application that encrypts the user's data and allows the users to be the decider of when their data is shared, and every time their data is used, users are required to consent. This way if an application tries to use a user's data, and the user is not using that application anymore, then the user can choose not to consent, and in that case ask for the deletion of their data.

This type of data privacy control will then remind the users of the different tech applications they have installed on their devices that they have not actively used. This way users can be proactive in requesting that their personal information be deleted before it is compromised.

User data collection can involve data on their geolocations, and many applications do collect user geolocation without a clear need on how this data enables their services or add value to the application. For most tech applications, users are not aware of their geolocation data collection especially when the tech application does not seem to need it. The tech application user consenting process requirement for specific user data utilization is critical both for user data privacy awareness and control because users can only control what they are aware of.

Users must be encouraged to consciously decide whether to share their personal data in tech applications. This is where the tech application value proposition will need to exceed the user valuation of their personal data based on privacy implications to command a thorough consideration of user data control.

The data encryption methodology can be used to deactivate or disable access to users' personal data until their next consent approval. The user data encryption methodology can enable the roadmap to data privacy control through surveying users' personal data view to determine which personal data is more critical for their data privacy considerations.

Based on users' inputs, machine learning models can be built to identify and flag the different kinds of personal data types available in smart cities which can be leveraged to accelerate users' notification rate and speed for faster responses. To quantify the user feedback, the federated learning technique can be used to aggregate user preferences on the different data privacy settings in regions based on cultural and geographical location for proper representation.

Data privacy levels can then be associated with aggregated user preferences compared to users' immediate privacy attributions. For example, if most users in a smart city choose to flag their profile pictures as being a privacy-sensitive element for the smart city, then every time someone tries to take and share a profile picture depicting them or upload the picture in a tech application or the web, they will receive a trigger to notify them based on the consensus of the privacy implications of the type of data and its contents to show that it is a privacy sensitive information and it carries privacy implications.

After the assessment, users can then be prompted to consent if they are still interested in sharing their data, otherwise, if users are not consciously consenting to provide their data, then it will be complicated in managing and controlling personal data that they are not even aware exists.

This will make it difficult to even track every time user data is used. Thus, through the user data privacy survey and the possibility of federated learning techniques, it is possible to provide an architectural framework and a redefinition of data submission on the web or in tech applications by enabling users' awareness and control of personal data just before they post it online. This approach helps provide an envelope of better user privacy-aware data communication for any post request that the users make on the web or in their mobile applications.

5.1. Privacy Awareness Application

The privacy awareness application has the objective of informing users of the different permissions that tech applications on their devices possess pertaining to the services being provided to them. It, therefore, compares the permissions acquired by the tech applications on users' devices and the expected information to be collected as outlined in tech applications' terms of service or software agreements to help users define what value they are gaining from tech application versus how much personal information they are providing in utilizing tech applications.

The privacy awareness application prototype created for this work queries all the applications installed on users' device and classify them as either system-installed applications or user-installed applications. System-installed applications refer to all pre-installed applications on users' devices that are present at the time of device acquisition or purchase.

Thus, user-installed applications mean that the user installed the tech application after the acquisition of the device. This implies that the users intended to get some value in installing the tech application in the first place, and as such, they need to understand the tradeoff as it pertains to their data privacy in using the tech application-provided services. In a nutshell, the privacy awareness application facilitates users' knowledge of what they need to know about the tech application's use of their personal information as they use and interact with them.

The privacy awareness application architecture is simplistic as users only need to click one button once to trigger the assessment, evaluation, and validation of the various user-installed applications regarding their use of users' personal data. The simple explanation of the application workflow is discussed, and both the simple and the more detailed application architectures are depicted in the figures presented in this chapter section. Figure 18 below depicts the simple architecture of the privacy awareness mobile application prototype that is developed through Android studio for the user interface frontend and Flask framework for the backend API server that does all the assessment and validation. The flask server API is deployed using the AWS lambda function for ease of query request analysis.

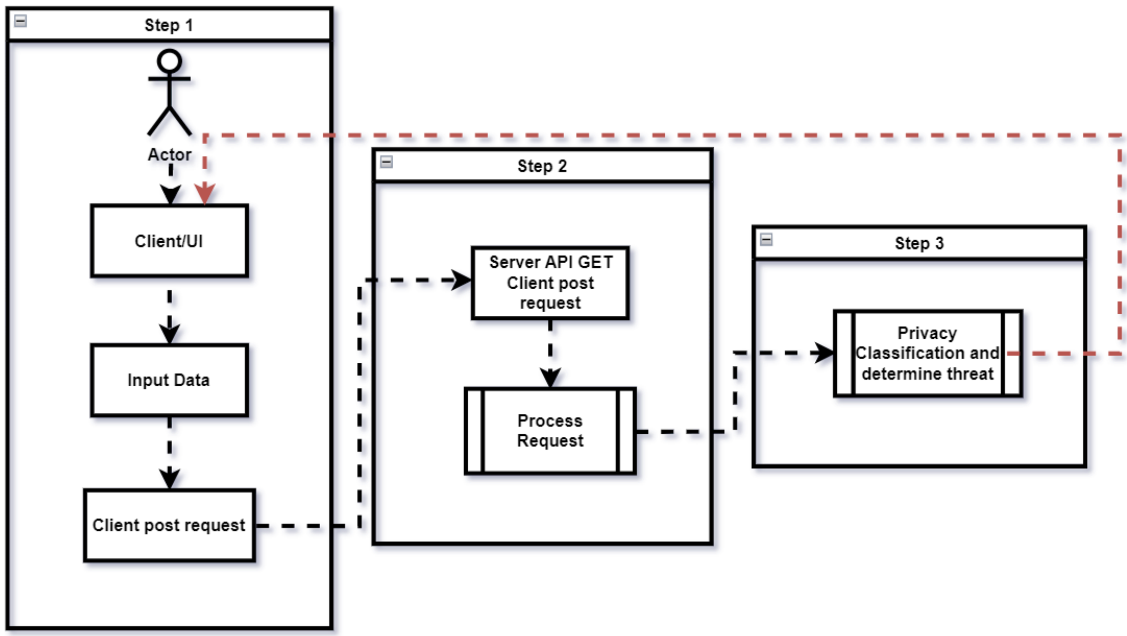

Step 1
Actor
Client/UI
Input Data
Client post request
Step 2
Server API GET Client post request
Process Request
Step 3
Privacy Classification and determine threat

Figure 18: The Simple Architecture of the Privacy Awareness Application

The privacy awareness application starts with the user engaging with it by launching its user interface and clicking the assessment button. The minute the button is clicked, the privacy awareness application queries and searches for all the user-installed applications together with all their granted permissions on the user's device using their package names. Once the search for all user-installed applications and their permissions are done, the application generates a request list object containing the list of all the user-installed applications and their respective granted permission.

The privacy awareness application on the user device or client then posts a request to the server application programming interface known as server API for further analysis of the device user-installed applications because the user device might not necessarily have enough computing power for the needed analysis. The server API is the cloud server that houses the application controller with the code to process the request appropriately given the list object containing user-installed applications and their permissions information.

Once the server API gets the client post request with the request list object, the processing of the request starts on the cloud server by parsing the list object and separating it into a list of list objects whereby each list contains one application with all its granted permissions on the user's device.

Now with the list of lists available, the server API parses each list and gets the application name from the application package name. With the application name identified, the server API fetches the application terms of use through web scraping via Google search. Once the link of the application's terms of use is found, the server API parses the application's terms of use and then evaluates it to determine the personal information the application collects and uses and the kinds of personal information that the application can consume.

Based on the tech data privacy survey, the different ratings are attributed to different personal data that users classified as being private or not are leveraged. The privacy ratings of the privacy awareness application prototype are based on how users responded to the survey questions as to how they consider the different types of personal information pertaining to them. Thus, with the attribution of the different personal data completed, the server API then calculates the overall privacy risk of the application based on the personal information it uses or can use.

The privacy risk is then normalized and turned into a percentage for easier report out to users as the privacy range will only vary from zero (non-private) to 1 (private). Once the privacy risk is determined for the application, the server API then assigns the privacy level to the application based on where its privacy risk falls on the scale from 0 percent to 100 percent. The privacy level range is subdivided into 3 zones, with the low privacy level spanning a privacy risk value of 0 to 33 percent, the medium privacy level spans a privacy risk value of 34 to 66 percent and finally, the high privacy level spans a privacy risk of 67 to 100 percent.

Once the privacy level is assigned to the application, the server API creates the privacy awareness application information dictionary and stores all the relevant data and findings about the application that was assessed, or it updates the already created privacy awareness application information dictionary with a new user-installed application assessment if more applications are installed on the user's device.

After the application completes assessing all the user-installed applications on the device and updates the privacy awareness application information dictionary, the saved privacy awareness application information dictionary is converted into a response list object that is sent back to the user interface which displays all the necessary information to the user after the analysis of all the user-installed applications in the list of lists object request is completed.

The server API controller assesses all the requested user-installed applications and returns the privacy assessment to the user to ensure the user is aware of any data privacy implications with their installed applications. The detailed privacy awareness application architecture and user interface are shown in figure 19 and figure 20 below respectively and outline granular steps for better algorithmic comprehension.

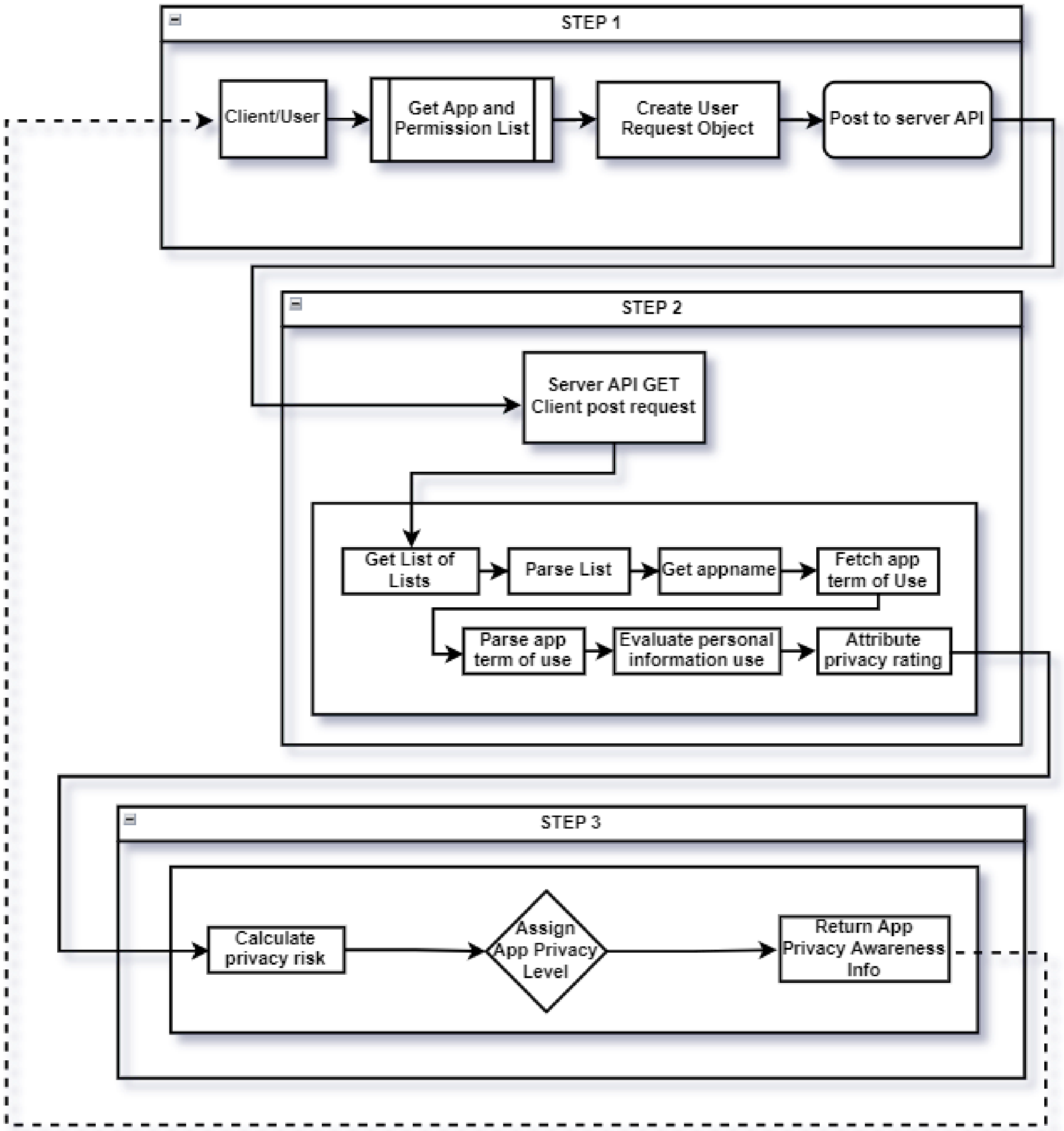
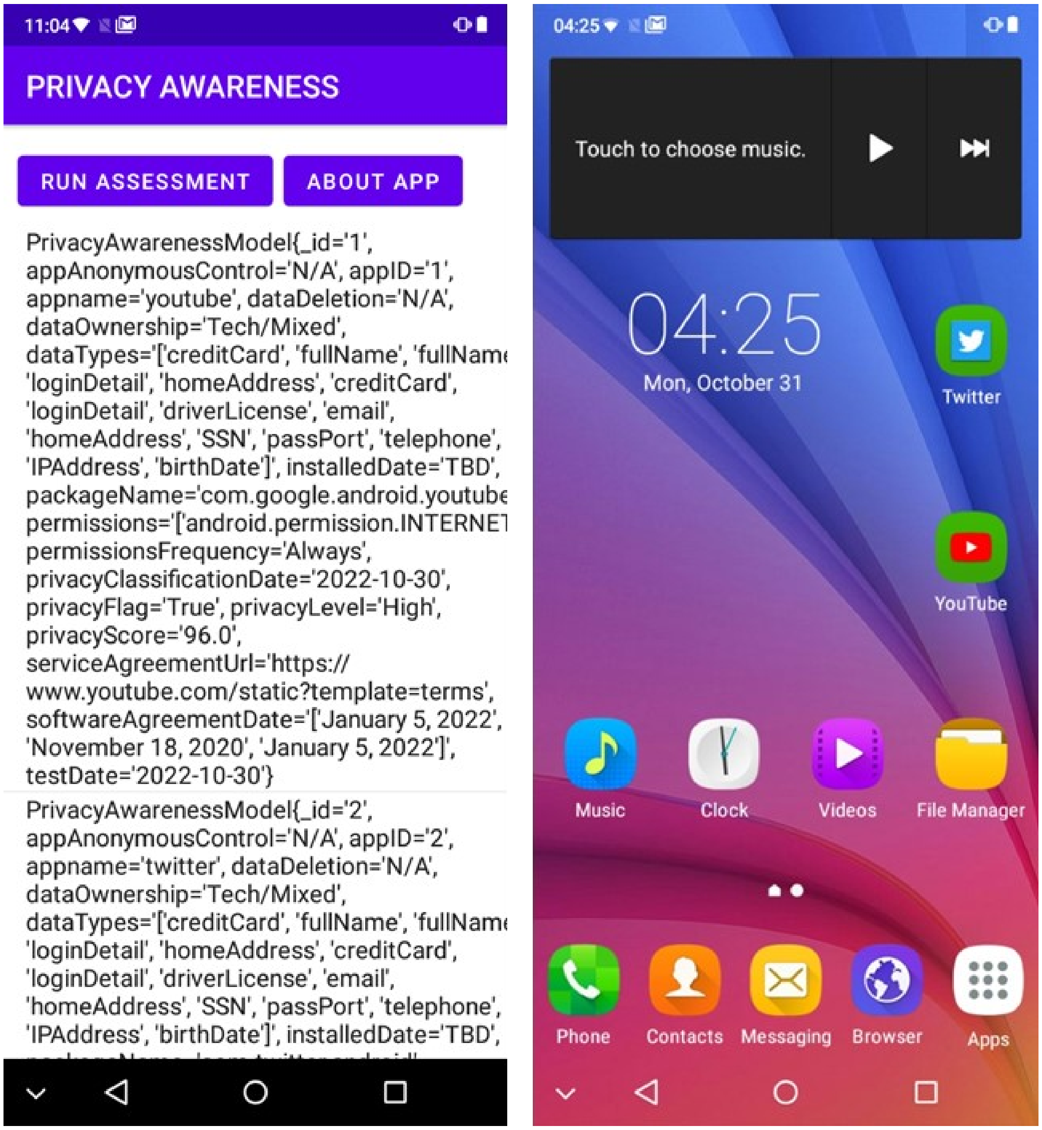


Figure 19: The Detailed Architecture of the Privacy Awareness Application



```
PrivacyAwarenessModel{_id='1',
appAnonymousControl='N/A', appID='1',
appname='youtube', dataDeletion='N/A',
dataOwnership='Tech/Mixed',
dataTypes='['creditCard', 'fullName', 'fullNam
'loginDetail', 'homeAddress', 'creditCard',
'loginDetail', 'driverLicense', 'email',
'homeAddress', 'SSN', 'passPort', 'telephone',
'IPAddress', 'birthDate']', installedDate='TBD',
packageName='com.google.android.youtube
permissions='['android.permission.INTERNET
permissionsFrequency='Always',
privacyClassificationDate='2022-10-30',
privacyFlag='True', privacyLevel='High',
privacyScore='96.0',
serviceAgreementUrl='https://
www.youtube.com/static?template=terms',
softwareAgreementDate='['January 5, 2022',
'November 18, 2020', 'January 5, 2022']',
testDate='2022-10-30'}
PrivacyAwarenessModel{_id='2',
appAnonymousControl='N/A', appID='2',
appname='twitter', dataDeletion='N/A',
dataOwnership='Tech/Mixed',
dataTypes='['creditCard', 'fullName', 'fullNam
'loginDetail', 'homeAddress', 'creditCard',
'loginDetail', 'driverLicense', 'email',
'homeAddress', 'SSN', 'passPort', 'telephone',
'IPAddress', 'birthDate']', installedDate='TBD',
```

Figure 20: The Privacy Awareness Mobile Application User Interface with Two User-installed Applications

5.2. Privacy Control Application

The privacy control application prototype has the objective to empower users with a real-time notification when their personally identifiable information (PII) is submitted on the web or in tech applications to better equip users to make sound decisions in sharing their PII data and giving them control of their personal data before their complete submission to the tech application databases. The privacy control application serves as a novel prototype for PII client-side validation that enables the privacy control framework that is discussed in this section.

The privacy control web application prototype consists of a frontend validation of input forms whereby the forms are validated for PII data and reported out to users in real-time to see if they still desire to submit their personal information. The privacy control web application prototype is created using Flask python framework for web application development, and it uses the madisonmay common regex python package found on GitHub under the following link (https://github.com/madisonmay/CommonRegex) to identify the different PPI information that is contained in the submitted text files or text input fields.

The privacy control web application prototype is deployed using the AWS lambda function, and it can be experimented with under the following link (https://r3eiil03xh.execute-api.us-east-1.amazonaws.com/dev).

As the information is flagged, the privacy rating of the form can be calculated in real-time based on the outcome of the tech data privacy survey to reflect how people consider data privacy as it pertains to their individual data.

Thus, the form would contain a placeholder that shows the personal information to be submitted or posted to the web application's backend. Therefore, based on the value of the web application services, the users can be the decider of consciously posting their PII data in tech applications.

The privacy control web application prototype application also addresses the data ownership concerns by allowing users to set the duration of the provided data in tech application databases as well as regulate the protocol of data usage beyond what is currently noted and highlighted in tech application terms of services.

Every form that is submitted with PII data should have two required fields that determine when the data should be deleted and how to communicate back to the owner when the data is transferred or used for other purposes respectively. These are frontend validation approaches that have been around for quite some time.

It is important to validate data input before they are posted in tech application databases and inform users of the potential PII data implication in their post request to serve both as a reminder and enabler for data privacy control. User data control lies in the ability of the user to be aware of their personal data and the implications of sharing it, as well as the ability to be empowered in deciding whether the data should be posted to receive the benefit provided by tech applications.

The privacy control framework proposed in this work is driving the idea of personally identifiable information validation in every post request or any form submission because this is the medium whereby users share their personal data over the internet. Therefore, to address the issue of user data privacy, it is paramount to have a way of validating PII data in post requests and form submissions to ensure that the PII data are taken care of appropriately with user-conscious consent. The only way users can control their personal data is by having mechanisms that notify them in real time whenever they want to entrust their personal data to someone else or another entity.

Thus, the front-end validation of PII data in submission forms is paramount to better enable users to participate in the protection of their private data and provide them control power to negotiate their own data policy pertaining to the value they are to receive from the tech applications. thus, the privacy control framework is used as a validation system without requiring users to know how it operates. Therefore, many PII validation can be built in for various data formats to detect PII data that users commonly share in submitting their personal data to the internet for various reasons.

The notification from the privacy control web application acts as a trigger for PII awareness in the data being submitted and triggers users' action to modify the data, cancel the post requests or form submissions, or provide additional information pertaining to customized data policy on how tech application makers should treat their personal data. The customized data policy may be in the form of reducing the length of data retention from the tech application databases or a request to be notified should the personal data be used for something else other than what it was intended for when the users submitted it.

The privacy control framework API consists of three main notions namely rules, rulesets, and validators, which can be expanded to incorporate external PII data validations from different techniques or machine learning models that tech application makers can easily leverage. The rules simply refer to the constraint that is assigned to a given data input field that is needed to be evaluated for PII data content.

The ruleset is an ensemble of all the rules available to validate PII data contained in any given data input field. The validator is the main method or engine that process the submitted input data and determine via various techniques whether the input data contains PII data, and flag or raise an exception to notify the user of the findings. Figure 21 below depicts a simple representation of the privacy control framework enabling the privacy control application.

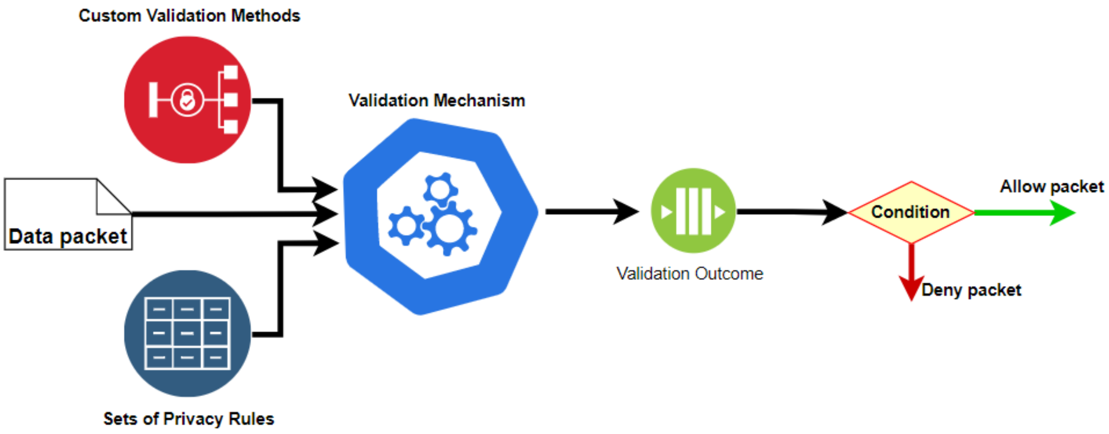


Figure 21: The Privacy Control Framework

Thus, with the help of the privacy control framework enabling the validation of personally identifiable data in users' submitted data input fields, the privacy control application is enabled. The privacy control application prototype makes use of three different input fields to help validate personally identifiable information in text data submitted by users.

The privacy control web application prototype is built with two different approaches; one with the madisonway common regex PII python packages and another with the pre-trained machine learning model "dbmdz/bert-large-cased-finetuned-conll03-english" pointing to revision "f2482bf" provided by Hugging Face under the following link (https://huggingface.co/dbmdz/bert-large-cased-finetuned-conll03-english) to help identify PII data using NLP BERT TensorFlow Token Classification machine learning model under transformers imported from pipeline, and demonstrate how PII validation can be expanded to greatly benefit users and even new data type formats.

The common regex PII python package and the NLP machine learning PII data detection were leveraged to accelerate the development of the privacy control web application prototype. The modest description of the privacy control web application prototype workflow is discussed following the simple architecture of the privacy control web application prototype depicted in figure 22 below.

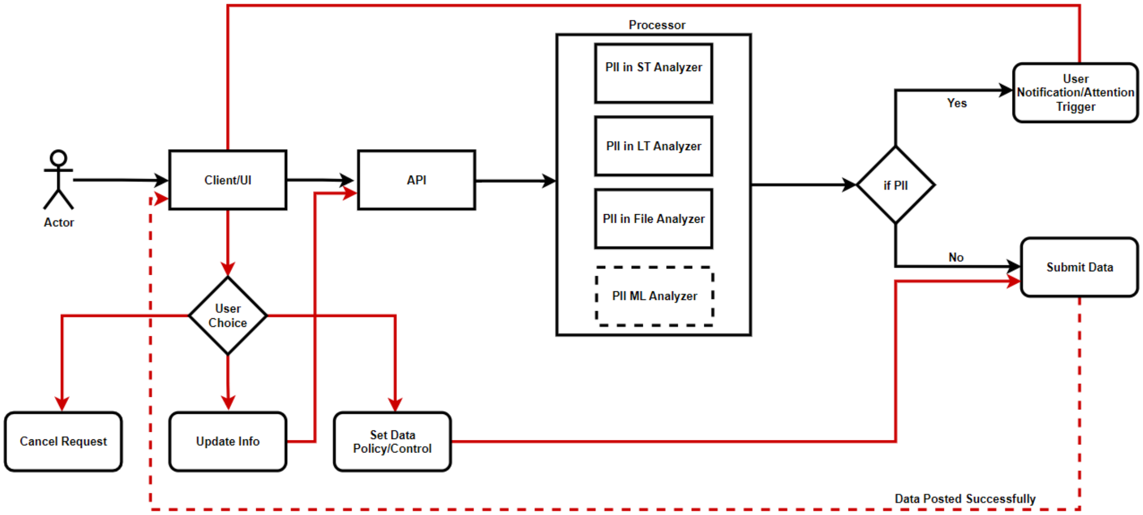


Figure 22: The Architecture of the Privacy Control Application

The privacy control web application starts with users engaging with the web application by browsing its domain name and filling in the form input fields with information that needs to be posted for a given service. Once the required field is completed and the users click the form submission button, a post request is created with the inputted data and sent to the server API for request processing.

The minute the server API receives the posted form, the privacy control web application controller begins to check and evaluate the validity of the posted data to ensure that it contains no PII data. The privacy control web application prototype validates the short text input field, long text input field, and text files submitted with “txt” and “pdf” extensions.

More data formats can be incorporated later to broaden the scope of PII detection and validity in user-submitted data in different kinds of tech applications. The privacy control web application controller invokes the different PII analyzers to validate that there are no PII data in the form submission in any of the text input fields. Figure 23 below depicts the user interface of the privacy control web application prototype.

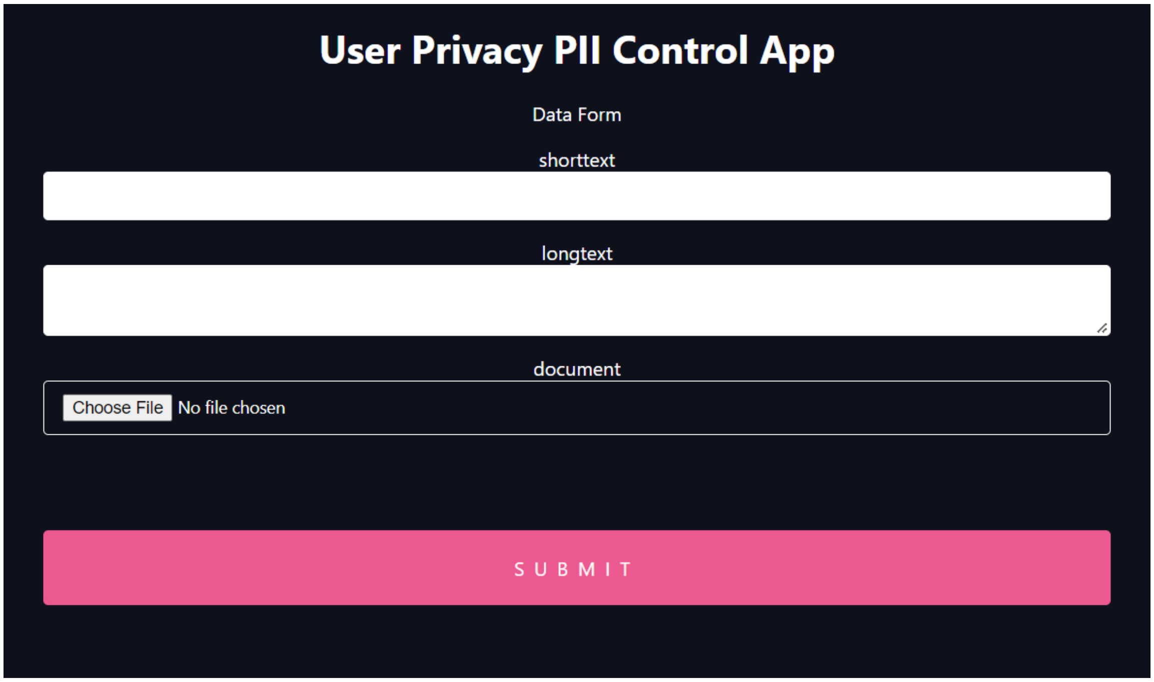


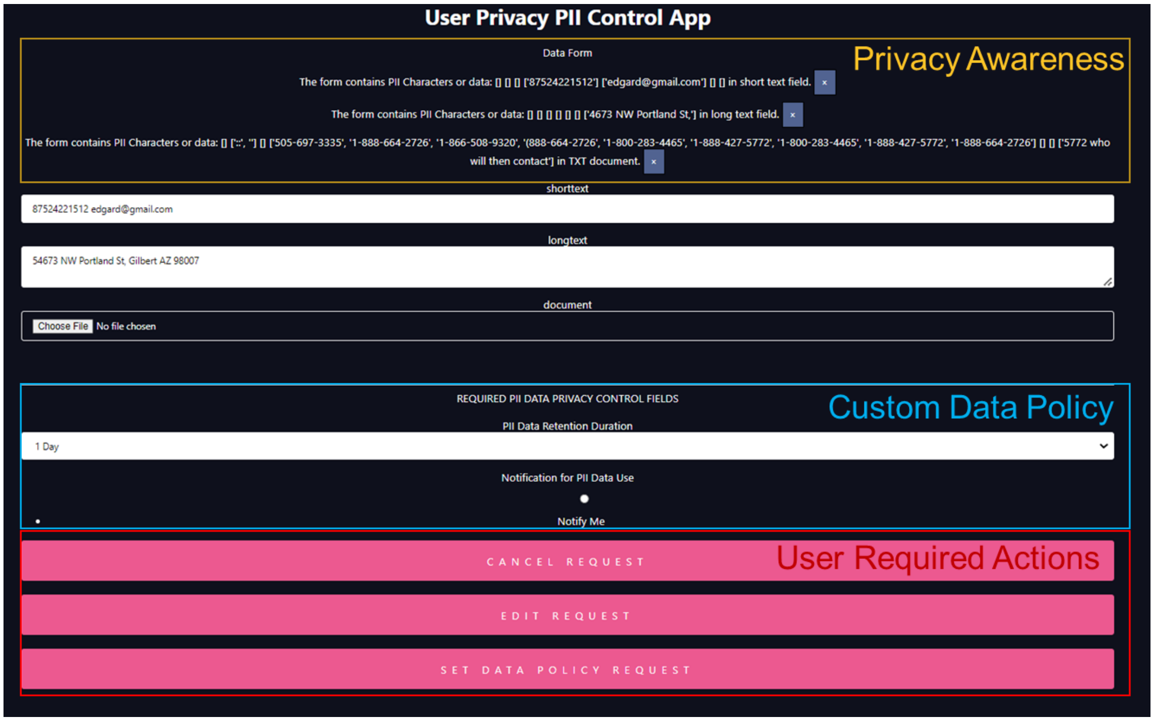
Figure 23: The User Interface of the Privacy Control Application

After the validation, if there are no PII data identified in the user request, then the data is successfully posted. However, if the data is deemed to possess PII data, the user is notified and provided action screens to help resolve the flag or control their PII data by setting up their own data policy. The privacy control web application notifies the user of the different PII flags in the inputted data and prompts the user to three actions namely to cancel the request, to update the information, and to set their PII data policy for the specific application. Thus, if the user chooses to cancel the request, then no form submission is completed.

Otherwise, users can update the information to remove PII information in the request and resubmit the form. If that is the case, the resubmitted form request goes through the validation again to verify that no PII data is flagged. However, if the user chooses to set their own data policy of the flagged data based on their needs, then additional data input fields are shown to them requiring them to set their custom data retention duration on the tech application databases, so that when the retention length is expired their personal data can be quickly moved to the deletion cycle of the tech application databases.

Likewise, the required field of notification is activated regarding the request for users to be notified to consent and approve whether their personal data can be used for anything else other than the purpose it was submitted for. Thus, anytime the user's personal data is used for other purposes, then users would be notified to reconsent for the new service or value.

Thus, when the user completes the additional required data field, their request is posted directly without validation as data control measures have been set in place. Figure 24 below depicts the user interface of the privacy control web application prototype showing real-time PII notifications for privacy awareness and control mechanisms related to user-needed actions.



User Privacy PII Control App

Data Form

The form contains PII Characters or data: [] [] [] ['87524221512'] ['edgard@gmail.com'] [] [] in short text field. ×

The form contains PII Characters or data: [] [] [] [] [] [] ['4673 NW Portland St,'] in long text field. ×

The form contains PII Characters or data: [] [':', ''] [] ['505-697-3335', '1-888-664-2726', '1-866-508-9320', '(888-664-2726', '1-800-283-4465', '1-888-427-5772', '1-800-283-4465', '1-888-427-5772', '1-888-664-2726'] [] [] ['5772 who will then contact'] in TXT document. ×

shorttext: 87524221512 edgard@gmail.com

longtext: 54673 NW Portland St, Gilbert AZ 98007

document: Choose File No file chosen

REQUIRED PII DATA PRIVACY CONTROL FIELDS

PII Data Retention Duration: 1 Day

Notification for PII Data Use

● Notify Me

Figure 24: Real-time PII Notifications for Privacy Awareness and Control.

CHAPTER 6

FUTURE RESEARCH

This dissertation opens many avenues of future research and interests that enrich the development of solutions that enable user PII data privacy control. As such, future research avenues span the following endeavors and interests that greatly benefit user awareness and control of personal data in tech applications. It is important to enable and expand on more customizable machine learning ML models to detect specific PII data in various contexts with different data formats from text, images, videos, and biometrics. This will enable more accurate detection of various PII data in user input, especially in unstructured data.

Another avenue of further research and implementation is investing in doing backend PII data validation and providing a way to characterize PII data that is submitted to ensure that it is handled appropriately. Furthermore, it is interesting to explore the backend PII data validation with dynamic database fields properties or attributes that possess the ability to trigger a notification to the source of data or users whenever data is used for something other than what the data was submitted for. The research would address another way to reconfigure tech application databases so that they do not just house static data but enable more dynamic data, meaning data that possesses content and methods for notifications when used.

Another avenue for future research is enabling edge-based or client-based storage of PII data for user control and using encryption methods to grant tech applications access to the PII data with an expiration date where PII data becomes corrupted even after they have been posted on the tech application databases. This research can help drive means of enabling one source of PII data that can be used to provide PII data to tech applications quickly and more reliably without losing control of it after it has been posted. With the edge-based or client-based storage approach, the users' PII data will be stored on their devices rather than in tech application databases, and tech applications will have to request access to the PII data whenever they want to use it just like tech applications request device location permissions.

Since PII data access and sharing is granted for a specific duration of time, the user can maintain control of personal data and be the decider to grant their PII data to tech application again whenever the copy of the PII data they possess becomes corrupted or expired. This will ensure a dynamic user-based data retention policy for the duration of service and value provision.

Another important future research is to enable the incorporation of federated learning techniques to aggregate user preference on what PII data they consider private and how it should be treated. This way geographical and cultural differences regarding PII data can be captured and incorporated for more relevant validation of users' inputs based on their immediate perspectives to avoid disagreements with users of different backgrounds. The federated learning technique will help gather anonymously the different data privacy ratings of how users view PII data and determine how private data can be considered and treated in a specific region.

The near future research avenue that is critical is to enable more PII data evaluation in all available data formats and sources that users interact with in different tech applications in submitting PII data online. Another future research opportunity and interest to pursue is the open-source deployment of various libraries or packages that enable tech application makers to leverage the user privacy control mechanisms to include in their application development to enable privacy by design with user data awareness and control.

Finally, it is fundamental to seek the enablement or inclusion of user PII data awareness and control as an additional pillar to the seven privacy-by-design principles. This requires that tech application makers find ways to inform users whenever their PII data is attempted to be posted to their API and provide definite user-triggered actions to ensure users remain in control of their PII data even after posting them.

This approach coupled with the future research endeavor discussed above ultimately encourages the enablement of less data retention on databases and more on edge devices for a more distributed secure system where the user decides what PII information to share and for how long.

CHAPTER 7

CONCLUSION

The concept and prototype of the privacy awareness application will enable and benefit the users to understand what is required of them in enabling privacy-aware tech data communication based on the services and value provided to them by tech applications. If the proposed value exceeds the importance of their private information, then the users can personally decide what is best for them to be able to deal with their data privacy control and control what tech applications are doing with their data.

Thus, by implementing these application prototypes, good privacy by design principles can be achieved and properly measured to especially allow the addition of empowering users to control their data regardless of when, where, and how they shared it. Considering the recent tech data privacy survey, the result shows that most people are in some forms, more in one way than others involved in using and interacting with tech applications for different reasons and different needs, and as such it is important to find technological ways to begin to address data privacy concerns in tech applications.

Therefore, this dissertation elaborates on the different steps needed to create a robust solution or remedy to data privacy concerns in tech applications in smart cities. As the survey shows that citizens are ready to play a role in being part of the solutions pertaining to their data privacy with proper awareness and control of their PII data in digital spaces. Through this research, users have been surveyed concerning tech applications to bring about awareness so users can limit the amount of personal information they share in tech applications because they have different levels of data security to protect the information because most of the information about users does not change over time.

It is paramount to find ways to determine how to collect PII data and for what purpose. This brings about the issue of the value of information and the value provided by the tech application that requires users to decide whether the value provided by the tech applications outweighs the value of the PII data they are providing in the long term. This forms an attempt to give users not only the control of when and where to share their personal information, but also the control to always provide consent when their PII data is being used beyond the blanket tech applications terms of use or software service agreements that nobody reads.

There are more data privacy risks in retaining personally identifiable data than in collecting it. If a protocol can be put in place to collect, use, and quickly delete personally identifiable data, then data privacy risk will be lessened. To minimize the data privacy risk, it is paramount to ensure that only minimal necessary personal data is collected to realize the service value of the tech applications and minimize the data retention length of PII data once the tech application service is enabled.

Users are willing to learn and understand how their PII data is used in tech applications and find out how they can play a role in controlling what their PII data is used for in tech applications. The current methods used by tech application makers of consent and terms of use are not effective, but they are rather ambiguous and not transparent enough for an average tech application user to understand. Since most users do not read these documents to fully understand how their data is used and what it enables, nor do any user know for sure which organizations constitute the third parties always mentioned in many tech applications' terms of use.

As such, this reality necessitates a reevaluation of how personally identifiable data should be handled in tech applications. This work, therefore, proposes user awareness mechanisms and approaches to give users control of their personal data to determine indeed whether they need to submit their PII data in return for the value they receive from the services that the tech applications enable for them.

This work is thorough in proposing a new way of submitting data by adding the control and awareness elements as the privacy control application shows in submitting PII data. PII data need to be evaluated in tech application forms, and if found in submitted forms, users must have control to set their own customized user-defined data policy. By data policy, it is implied that data retention duration can be set and request for personal notification be attached to the PII data for any use outside the scope of its provision.

It is evident in smart cities today, that tech applications have embarked on blanket notifications of their terms of use agreement's revisions or updates, with the reality that most users do not read these agreements, and as such user data is being used without users' real and conscious consent. Therefore, users need to be notified only explicitly when their PII data is being used or considered rather than in general.

This way users will be players in the tech application data privacy solution space to ensure that the privacy-by-design methodologies are well implemented with the constant feedback of the users. This will require user awareness of what data privacy concerns are, and the different damages they cause to their confidentiality and digital identification. It is key that users are involved and aware because they get to decide based on the tech services, they use how their PII data is handled to minimize the risk of data compromission.

Thus, this work opens a new field of research on how to give tech application users control of their personal data, so that they can be the decider of the data policy that pertains to their PII data as the tech data privacy survey showed to reveal that users have different information about themselves that they consider more private than others. Tech application makers need to welcome users as definite deciders on how their PII data should be handled. This work aimed to use technology to solve most of the issues about tech application data privacy proactively so that users are not disturbed and overwhelmed every time by unknown and unauthorized tech applications.

REFERENCES

[1] 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.

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

[3] 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.

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

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] Mohanty, Saraju. (2016). Everything You Wanted to Know About Smart Cities. IEEE Consumer Electronics Magazine. 5. 60-70. 10.1109/MCE.2016.2556879.

[11] Hahn, Dalton & Munir, Arslan & Behzadan, Vahid. (2019). Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. IEEE Intelligent Transportation Systems Magazine. PP. 1-1. 10.1109/MITS.2019.2898973.

[12] Cucchiara, Rita. (2005). Multimedia surveillance systems. 3-10. 10.1145/1099396.1099399.

[13] Gupta, B B & Yamaguchi, Shingo & Agrawal, Dharma. (2017). Advances in Security and Privacy of Multimedia Big Data in Mobile and Cloud Computing. Multimedia Tools and Applications. 1-6. 10.1007/s11042-017-5301-x.

[14] Adams, Anne & Sasse, Angela. (2001). Privacy in Multimedia Communications: Protecting Users, Not Just Data. 10.1007/978-1-4471-0353-0_4.

[15] Carsten Maple (2017) Security and privacy in the internet of things, Journal of Cyber Policy, 2:2, 155-184, DOI: 10.1080/23738871.2017.1366536

[16] Noda, K., Hashimoto, N., Nakadai, K., & Ogata, T. (2015). Sound source separation for robot audition using deep learning. 2015 IEEE-RAS 15th International Conference on Humanoid Robots (Humanoids), 389-394.

[17] Jaiswal, Mimansa & Mower Provost, Emily. (2020). Privacy Enhanced Multimodal Neural Representations for Emotion Recognition. Proceedings of the AAAI Conference on Artificial Intelligence. 34. 7985-7993. 10.1609/aaai.v34i05.6307.

[18] Wang, Junjue & Amos, Brandon & Das, Anupam & Pillai, Padmanabhan & Sadeh, Norman & Satyanarayanan, Mahadev. (2017). A Scalable and Privacy-Aware IoT Service for Live Video Analytics. 38-49. 10.1145/3083187.3083192.

[19] Prabhakar, Salil & Pankanti, S. & Jain, Anil. (2003). Biometric Recognition: Security and Privacy Concerns. Security & Privacy, IEEE. 1. 33 - 42. 10.1109/MSECP.2003.1193209.

[20] Evans, Nicholas & Marcel, Sebastien & Ross, Arun & Teoh, Andrew. (2015). Biometrics Security and Privacy Protection From the Guest Editors]. Signal Processing magazine IEEE. 32. 17-18. 10.1109/MSP.2015.2443271.

[21] Pirinen, Pekka. (2014). A Brief Overview of 5G Research Activities. 10.4108/icst.5gu.2014.258061.

[22] Dangi, R., Lalwani, P., Choudhary, G., You, I., & Pau, G. (2021). Study and Investigation on 5G Technology: A Systematic Review. Sensors (Basel, Switzerland), 22(1), 26. https://doi.org/10.3390/s22010026

[23] Perspectives on 5G applications and services. (2022). IEEE Future Networks. https://futurenetworks.ieee.org/roadmap/perspectives-on-5g-applications-and-services#:~:text=5G%20has%20the%20potential%20to,new%20applications%20for%20mobile%2C%20eHealth%2C

[24] Agiwal, M.; Roy, A.; Saxena, N. Next generation 5G wireless networks: A comprehensive survey. IEEE Commun. Surv. 2016, 18, 1617–1655.

[25] Buzzi, S.; Chih-Lin, I.; Klein, T.E.; Poor, H.V.; Yang, C.; Zappone, A. A survey of energy-efficient techniques for 5G networks and challenges ahead. IEEE J. Sel. Areas Commun. 2016, 34, 697–709.

[26] E. Musafiri Mimo & T. McDaniel. (2021) Security Concerns and Citizens' Privacy Implications in Smart Multimedia Applications. Smart Multimedia 2021: Not Yet Published.

[27] Serrano, Will. (2021). Big Data in Smart Infrastructure. 10.1007/978-3-030-55187-2_51.

[28] AJ Abdallat. (2021). How will artificial intelligence power the cities of Tomorrow? RSS. https://eandt.theiet.org/content/articles/2021/09/how-will-artificial-intelligence-power-the-cities-of-tomorrow/

[29] Gartner_Inc. (2022). Three rules when using AI to add value to your IoT smart cities. Gartner. https://www.gartner.com/en/documents/3870008

[30] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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

[37] 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.

[38] 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

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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

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

[45] 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

[46] 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/.

[47] 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.

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

[49] 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/.

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

[51] 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

[52] 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

[53] M. Sookhak, H. Tang, Y. He and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Second quarter 2019, doi: 10.1109/COMST.2018.2867288.

[54] Mimo, E. M., & Mcdaniel, T. (2021). 3D Privacy basis: The Citizen Value Driven Privacy basis. In 2021 IEEE International Smart Cities Conference, ISC2 2021 (2021 IEEE International Smart Cities Conference, ISC2 2021). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ISC253183.2021.9562841

[55] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in 2010 IEEE Symposium on Security and Privacy. Berkeley, CA, USA: IEEE, May 2010, pp. 447–462.

[56] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of Resource Constrained Devices in the Internet of Things," IEEE Communications Magazine, vol. 50, no. 12, pp. 144–149, December 2012.

[57] Chen, Hanchun & Yang, Yongjie. (2018). A Practical Scheme of Smart Grid Privacy Protection. IOP Conference Series: Materials Science and Engineering. 394. 042058. 10.1088/1757-899X/394/4/042058.

[58] Hoque, Shahidul & Rahim, Aneel & Cerbo, Francesco. (2014). Smart Grid Data Anonymization for Smart Grid Privacy. 470. 10.1007/978-3-319-12574-9_8.

[59] Singh, Parminder & Masud, Mehedi & Hossain, M. Shamim & Kaur, Avinash. (2021). Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid ☆. Computers & Electrical Engineering. 93. 10.1016/j.compeleceng.2021.107209.

[60] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," Vehicular Communications, vol. 1, no. 2, pp. 53–66, April 2014.

[61] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks. Montreal, Quebec, Canada: ACM, September 2007, pp. 19–28.

[62] S. Yip, K. Wong, R. C. -. Phan, S. Tan, I. Ku and W. Hew, "A Privacy-Preserving and Cheat-Resilient electricity consumption reporting Scheme for smart grids," 2014 International Conference on Computer, Information and Telecommunication Systems (CITS), 2014, pp. 1-5, doi: 10.1109/CITS.2014.6878971.

[63] A. Lee and T. Brewer. 2009. Smart grid cyber security strategy and requirements, US Department of Commerce, Draft Interagency Technical Report NISTIR 7628. National Institute of Standards and Technology (NIST): Gaithersburg, MD.

[64] Otuoze, Abdulrahaman & Mustafa, Mohd & Larik, Raja Masood. (2018). Smart grids security challenges: Classification by sources of threats. 5. 468-483. 10.1016/j.jesit.2018.01.001.

[65] Pereira, Gabriela & Parycek, Peter & Falco, Enzo & Kleinhans, Reinout. (2018). Smart governance in the context of smart cities: A literature review. Information Poli-ty. 23. 1-20. 10.3233/IP-170067.

[66] Scholl, H. J., & AlAwadhi, S. (2016b). Smart governance as key to multi-jurisdictional smart city initiatives: The case of the eCityGov Alliance. Social Science Information, 55(2), 255-277. doi: https://doi.org/10.1177/0539018416629230.

[67] Goel S., Hong Y. (2015) Security Challenges in Smart Grid Implementation. In: Smart Grid Security. Springer Briefs in Cybersecurity. Springer, London. https://doi.org/10.1007/978-1-4471-6663-4_1

[68] Mimo, E. M., & McDaniel, T. (2022). Smart Cities: A Survey of Tech-Induced Privacy Concerns. In Advanced Sciences and Technologies for Security Applications (pp. 1-22). (Advanced Sciences and Technologies for Security Applications). Springer. https://doi.org/10.1007/978-3-031-04424-3_1

[69] Arca, Sevgi & Hewett, Rattikorn. (2020). Privacy Protection in Smart Health. 1-8. 10.1145/3406601.3406620.

[70] Jagadeesh, Ranjith & Mahantesh, Dr. (2019). Privacy and Security issues in Smart Health Care. 378-383. 10.1109/ICEECCOT46775.2019.9114681.

[71] Murphy, Maria Helen. (2018). Pseudonymisation and the smart city: Considering the General Data Protection Regulation. 10.4324/9781351182409-14.

[72] Paiva, Sara & Ahad, Mohd & Zafar, Sherin & Tripathi, Gautami & Khalique, Aqeel & Hussain, Imran. (2020). Privacy and security challenges in smart and sustainable mobility. SN Applied Sciences. 2. 10.1007/s42452-020-2984-9.

[73] Samih, Haitham. (2019). Smart cities and the internet of things. Journal of Information Technology Case and Application Research. 21. 1-10. 10.1080/15228053.2019.1587572.

[74] J. M. d. Fuentes, A. I. Gonzalez-Tablas, and A. Ribagorda, “Overview of Security Issues in Vehicular Ad-Hoc Networks,” 2010.

[75] Staff, CACM. (2016). Future cyberdefenses will defeat cyberattacks on PCs. Communications of the ACM. 59. 8-9. 10.1145/2963167.

[76] J. B. Kenney, “Dedicated Short-Range Communications (DSRC) Standards in the United States,” Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, July 2011.

[77] Klimburg, Alexander. (2011). Mobilising Cyber Power. Survival. 53. 10.1080/00396338.2011.555595.

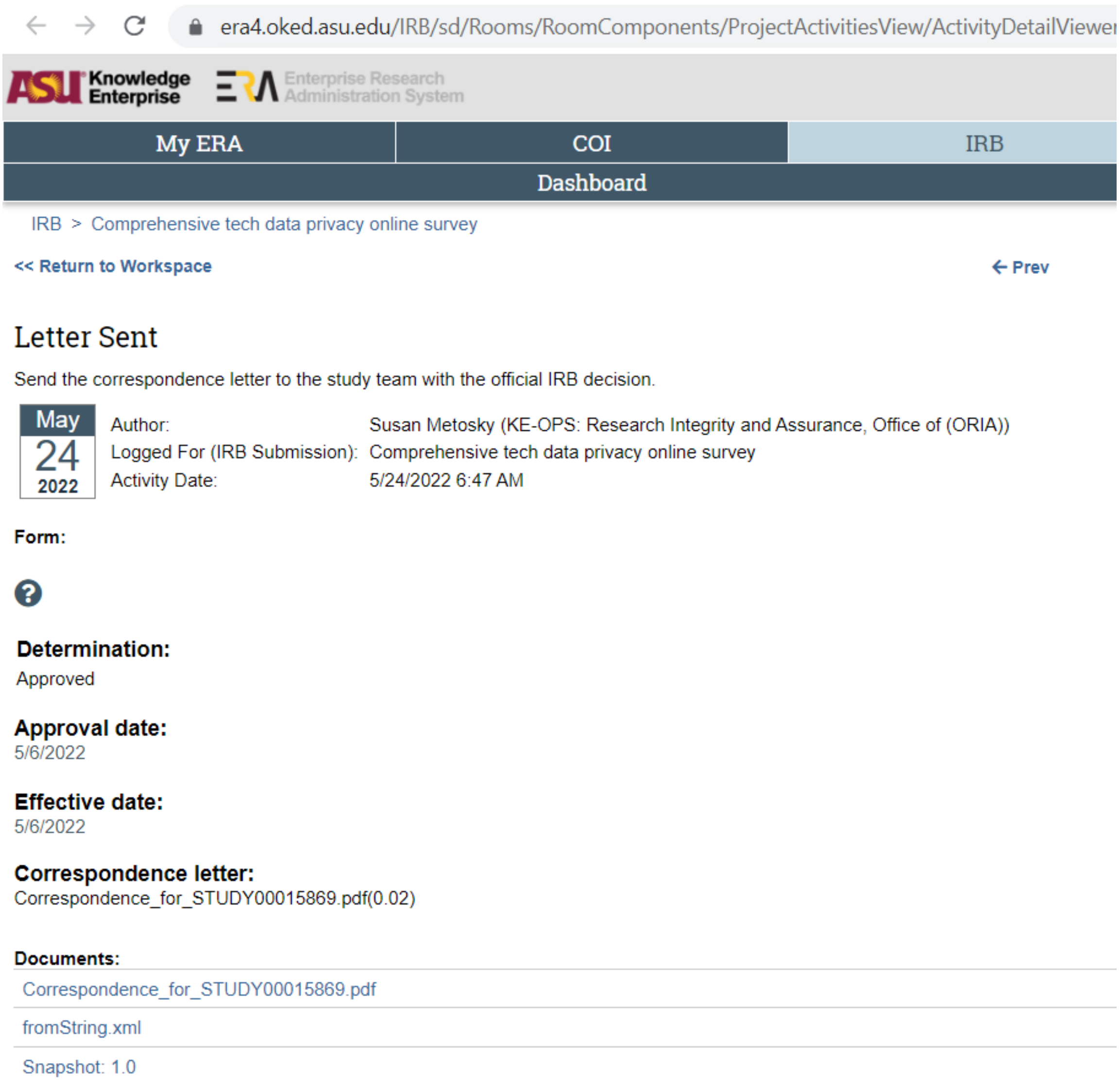
[78] Aleisa, Noura & Renaud, Karen. (2017). Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions. 198-205. 10.5220/0006233701980205.

[79] Cavoukian, A. (2010). Privacy by Design: The 7 Foundational Principles (Revised: Oktober 2010)

[80] Zhang, H., Xu, L., Lin, L., Wang, X. (2020). De-anonymizing Social Networks with Edge-Neighborhood Graph Attacks. In: Yu, S., Mueller, P., Qian, J. (eds) Security and Privacy in Digital Economy. SPDE 2020. Communications in Computer and Information Science, vol 1268. Springer, Singapore. https://doi.org/10.1007/978-981-15-9129-7_49

APPENDIX A

IRB APPROVAL \


era4.oked.asu.edu/IRB/sd/Rooms/RoomComponents/ProjectActivitiesView/ActivityDetailViewer
ASU Knowledge Enterprise
ERA Enterprise Research Administration System
My ERA
COI
IRB
Dashboard
IRB > Comprehensive tech data privacy online survey
<< Return to Workspace
← Prev

Letter Sent

Send the correspondence letter to the study team with the official IRB decision.

May 24 2022	Author:	Susan Metosky (KE-OPS: Research Integrity and Assurance, Office of (ORIA))
	Logged For (IRB Submission):	Comprehensive tech data privacy online survey
	Activity Date:	5/24/2022 6:47 AM

Form:

?

Determination:
Approved

Approval date:
5/6/2022

Effective date:
5/6/2022

Correspondence letter:
Correspondence_for_STUDY00015869.pdf(0.02)

Documents:

Correspondence_for_STUDY00015869.pdf

fromString.xml

Snapshot: 1.0

APPENDIX B

TECH APPLICATIONS DATA PRIVACY SURVEY QUESTIONNAIRE

1. What is your gender?

Male
Female
Prefer not to answer

2. What is your race?

Black or African American
White
American Indian or Alaska Native
Asian
Native Hawaiian or Other Pacific Islander.
Prefer not to answer

3. What is your age range?

Under 20
20 - 29
30 - 39
40 - 49
50 - 59
60 - 69
70 - 79
80 - 89
90 - 99
Over 100

4. What is your Email address?

5. What is your employment status?

Unemployed
Self-Employed
Employed

6. What is your work’s status?

Student
Full-time worker
Entrepreneur
Part-time worker
Looking for work
Unable to work

7. What is your current city location?

8. What is your Marital status?

Single
Married
Divorced
Separated
Widowed

9. What is your nationality or citizenship?

10. What is your place of birth?

11. What is your date of birth?

12. What is your salary range (gross income per year)?

Under $15000
Between $15000 and $29999
Between $30000 and $49999
Between $50000 and $74999
Between $75000 and $99999
Between $100000 and $149999
Between $150000 and $199999
Between $200000 and $249999
Between $250000 and $299999
Between $300000 and $349999
Between $350000 and $399999
Over $400000

13. What is your highest level of education?

High school diploma
GED
Associate degree
Bachelor’s degree
Master’s degree
Doctorate degree
Self-taught

14. How many children do you have?

None
One

Two
Three
Four
Five or More

15. How often do you think your privacy is preserved while online over the internet?

Never
Rarely
Usually
Always
Other (please specify)

16. How often do you provide your personal information to access or use any application on the internet?

Once a week
Once a month
Once a quarter
Twice a month
Other (please specify)

17. How often do you ensure and enforce security while using online applications over the internet by ensuring your firewall is set on and antivirus active?

Never
Rarely
Usually
Always
Other (please specify)

18. How often do you use your mobile device to access your banking apps?

Once a week
Once a month
Once a quarter
Twice a month
Other (please specify)

19. How often do you use your mobile device to access your social media apps?

Once a week
More than once a week
Once a month
More than once a month

Once a quarter
More than one a quarter
Other (please specify)

20. Which social media apps do you use more than five times a week? Select

Facebook
YouTube
Instagram
WhatsApp
Snapchat
TikTok
Add any other
Other (please specify)

21. Which media streaming apps do you use more than three times a week?

Facebook
YouTube
Instagram
TikTok
Netflix
Hulu
Spotify
Pandora
Sound cloud
iTunes
Add any other

22. Which money transfer apps do you use more than once a month?

Cash App
Venmo
PayPal
MoneyGram
Western Union
Walmart Ria
Zelle
Other (please specify)

23. Which online banking apps do you often use?

USBank
Chase
Wells Fargo

Bank of America
Prefer not to answer
Add any other
Other (please specify)

24. Do you use online banking apps more than your local bank branch or ATM for your banking needs?

Yes
No

25. How often do you visit your local bank branch or ATM for your banking needs?

Once a week
Once a month
Once a quarter
Twice a month
Other (please specify)

26. Which media streaming apps do you use for more than 15 minutes a day?

Facebook
YouTube
Instagram
TikTok
Netflix
Hulu
Spotify
Pandora
Sound cloud
iTunes
Add any other
Other (please specify)

27. Which Location or direction apps do you use more than once a month?

Google maps
Uber
Add any other
Other (please specify)

28. Which social media apps do you use more than once a day?

Facebook
YouTube

Instagram
WhatsApp
Snapchat
TikTok
Other (please specify)
None of the above

29. Which eCommerce apps do you use more than once a month?

eBay
Amazon
Facebook Marketplace
Craigslist
Walmart
Best buy
Home Depot
Target
Costco
Add any other
Other (please specify)

30. How often do you sign into other apps using your social media credential?

Never
Rarely
Usually
Always
Other (please specify)

31. How do you sign into other apps?

Using Gmail credentials
Using Facebook credentials
Using other social media apps credentials
Using normal email password credentials
Add any other
Other (please specify)

32. How often do you share your image or picture on social media/apps?

Never
Rarely
Usually
Always
Other (please specify)

33. How often do you share your audio clips on social media/apps?

Never
Rarely
Usually
Always
Other (please specify)

34. How often do you share your video clips on social media/apps?

Never
Rarely
Usually
Always
Other (please specify)

35. How often do you share images or pictures where you can be identified on social media/apps?

Never
Rarely
Usually
Always
Other (please specify)

36. How often do you share videos where you can be identified or heard on social media/apps?

Never
Rarely
Usually
Always
Other (please specify)

37. How often do you share audio clips where you can be heard on social media/apps?

Never
Rarely
Usually
Always
Other (please specify)

38. How often do you think about being recorded/on tape with or without your consent?

Never
Rarely
Usually
Always
Other (please specify)

39. How often do you video chat or call on social media?

Never
Rarely
Usually
Always
Other (please specify)

40. How often do you allow apps to access and control your mobile device microphone?

Never
Rarely
Usually
Always
Other (please specify)

41. How often do you allow apps to access and control your mobile device camera?

Never
Rarely
Usually
Always
Other (please specify)

42. How often do you allow apps to access your mobile device location?

Never
Rarely
Usually
Always
Other (please specify)

43. How often do you allow google maps to access your mobile device's current location?

Only while using the app
All the time
Never
Rarely
Usually

Other (please specify)

44. How often do you allow answer calls from unknown numbers?

Once a day
Multiple times a day
Once a week
Multiple times a week
Once a month
Multiple times a month
Other (please specify)

45. How often do you reject block phone calls from unknown numbers?

Once a day
Multiple times a day
Once a week
Multiple times a week
Once a month
Multiple times a month
Other (please specify)

46. How often do you block unknown phone numbers?

Once a day
Multiple times a day
Once a week
Multiple times a week
Once a month
Multiple times a month
Other (please specify)

47. Do you have concerns when unknown numbers call you for solicitations?

Never
Rarely
Usually
Always
Other (please specify)

48. How concerned are you with your information being sold to third parties?

Never
Rarely
Usually

Always
Other (please specify)

49. How often do you block or uninstall applications wanting to control your device's microphone?

Never
Rarely
Usually
Always
Other (please specify)
50. How often do you block or uninstall applications wanting to control your device's camera?

Never
Rarely
Usually
Always
Other (please specify)

51. Which of the following information do you consider private?

Full name
Home address
Email address
Date of birth
Telephone number
Social security number
Passport number
Driver's license number
Credit card numbers
Owned properties e.g. vehicle identification number (VIN)
Login details
Processor or device serial number*
Media access control (MAC)*
Internet Protocol (IP) address*
Device IDs*
Cookies*
Biological Biometrics data (fingerprints, face, iris, veins, etc.)
Behavioral Biometrics data (keystroke dynamics, gait, signature, voice, etc.)
Other (please specify)

52. Which of the following do you share?

First name

Last name (if common)
Country, state, city, zip code
Gender
Race
Non-specific age (e.g. 30-40 instead of 30)
Job position and workplace

53. Which of the following do you share, control, or delete?

transaction history
devices IP addresses
browser history
posts on social media

54. Which of the following frameworks or institutions do you know or heard of?

The U.S. Privacy Act, which governs how to collect, maintain, use, and disseminate PII
The Health Insurance and Portability Act (HIPAA) governing patient privacy
The Children's Online Privacy Protection Act (COPPA), is designed to protect the personal information of children under the age of 13
None of the above
All the above

55. Which of the following organizations do you know?

The Federal Trade Commission (FTC) and its Department of Consumer Protection
Local Departments of Consumer Affairs
The Federal Communications Commission (FCC)
The National Institute of Standards and Technology (NIST)
The Network Advertising Initiative (NAI), a self-regulatory organization
None of the above
All the above

56. How often do you provide your full name information online, in apps, or for services over the internet?

Never
Rarely
Usually
Always
Other (please specify)

57. How often do you ask for your personal information to be deleted from online applications or service applications over the internet?

Never
Rarely
Usually
Always
Other (please specify)

58. Which of the following information have you shared online or in applications?

Full name
Home address
Email address
Date of birth
Owned properties e.g. vehicle identification number (VIN)
Login details

59. Which of the following information have you shared online or in applications?
Telephone number
Social security number
Passport number
Driver’s license number
Credit card numbers

60. Which of the following information have you shared online or in applications?
Biological Biometrics data (fingerprints, face, iris, veins, etc.)
Behavioral Biometrics data (keystroke dynamics, gait, signature, voice, etc.)
Fingerprints
Face
Iris
Veins
Keystroke dynamics
Gait
Signature
Voice
Other (please specify)

61. Which of the following information do you care about while online or using applications?
Processor or device serial number
Media access control (MAC)
Internet Protocol (IP) address
Device IDs
Cookies
None of the above
All the above

62. Which of the following information have you shared online for specific services over the internet?

Full name
Home address
Email address
Date of birth
Owned properties e.g. vehicle identification number (VIN)
Login details
None of the above
All the above

63. Which of the following information have you shared online for specific services over the internet?
Telephone number
Social security number
Passport number
Driver's license number
Credit card numbers
None of the above
All the above

64. Which of the following Biometrics information have you shared online for specific services over the internet?
Fingerprints
Face
Iris
Veins
Keystroke dynamics
Gait
Signature
Voice
Other (please specify)

65. Which of the following information do you accept from your browser to access online or over the internet when prompted?
Processor or device serial number
Media access control (MAC) address
Internet Protocol (IP) address
Device IDs
Cookies
Other (please specify)

66. Which of the following information do you actively avoid sharing online?

Full name
Home address
Email address
Social security number
Passport number
Driver’s license number
Credit card numbers
Date of birth
Telephone number
Owned properties e.g. vehicle identification number (VIN)
Login details
Processor or device serial number*
Media access control (MAC)*
Internet Protocol (IP) address*
Device IDs*
Cookies*
Biological Biometrics data (fingerprints, face, iris, veins, etc.)
Behavioral Biometrics data (keystroke dynamics, gait, signature, voice, etc.)
Other (please specify)

67. Which money transfer apps do you use more than once a month?

Cash App
PayPal
MoneyGram
Western Union
Walmart Ria
YouTube
iTunes
Add any other
Other (please specify)

68. Which media streaming apps do you use more than once a day?

Facebook
YouTube
Instagram
Netflix
Hulu
Spotify
Pandora
Sound Cloud
iTunes

Add any other
Other (please specify)

69. How often do you refuse to consent to software or online applications for services over the internet?

Never
Rarely
Usually
Always
Other (please specify)

70. Would you wish to have an application that grants you control of your private information and notify you whenever your private information is being used or requested in applications or over the internet?

Yes
No

71. Which eCommerce apps do you use more than twice a month?

eBay
Amazon
Facebook Marketplace
craigslist
Walmart
Best buy
Home Depot
target
Add any other
Other (please specify)

72. How often do you support organizations that aim to reinforce the preservation of citizens' privacy online?

Never
Rarely
Usually
Always
Other (please specify)

73. How often have you been affected by a potential cyber-attack in online applications and over the internet?

Never

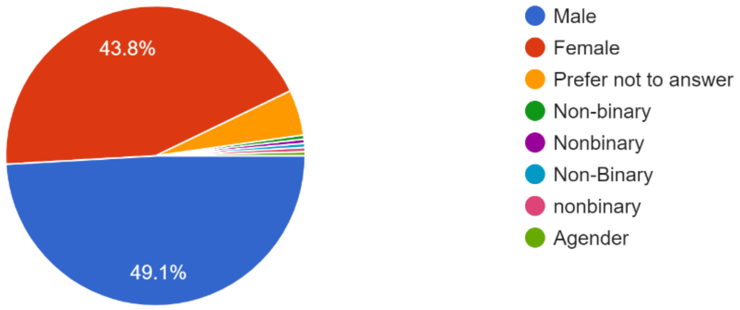
Rarely
Usually
Always
Other (please specify)

APPENDIX C

KEY SURVEY RESULTS SUMMARY

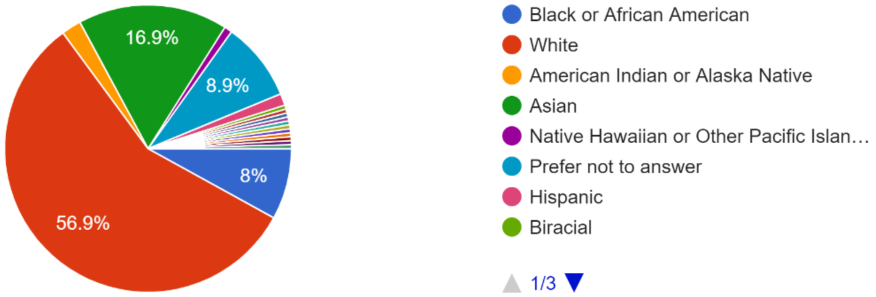
What is your gender?

224 responses



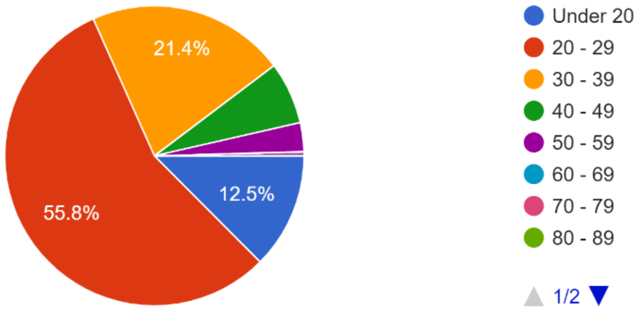
What is your race?

225 responses



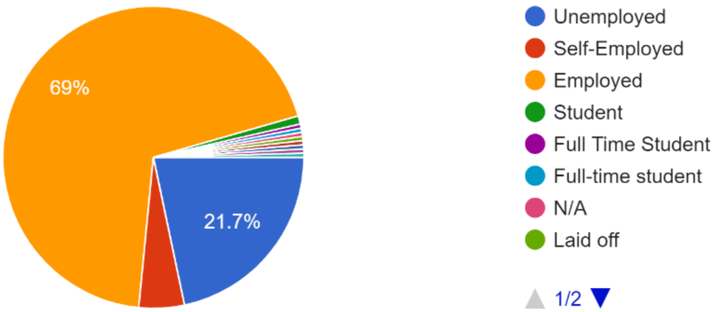
What is your age range?

224 responses



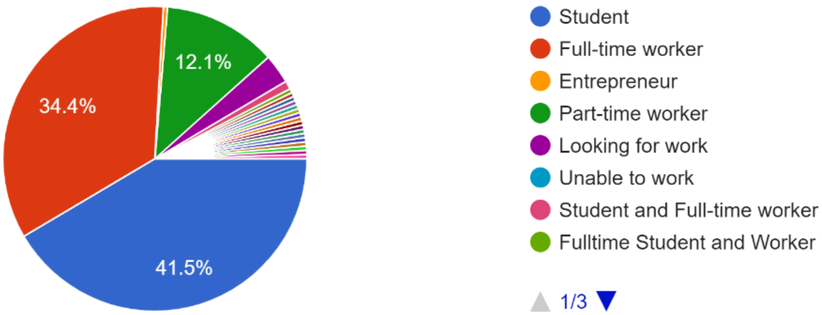
What is your employment status?

226 responses



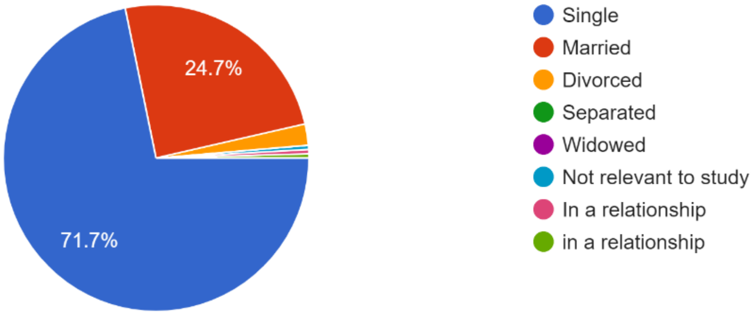
What is your work's status?

224 responses



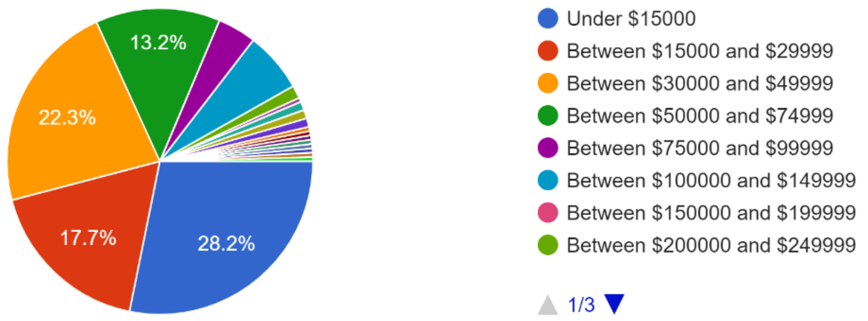
What is your Marital status?

223 responses



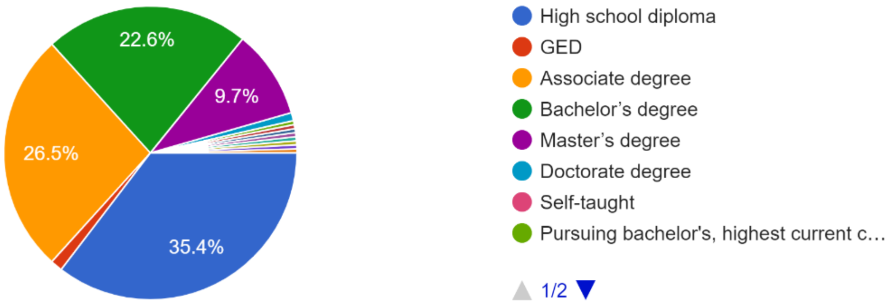
What is your salary range (gross income per year)?

220 responses



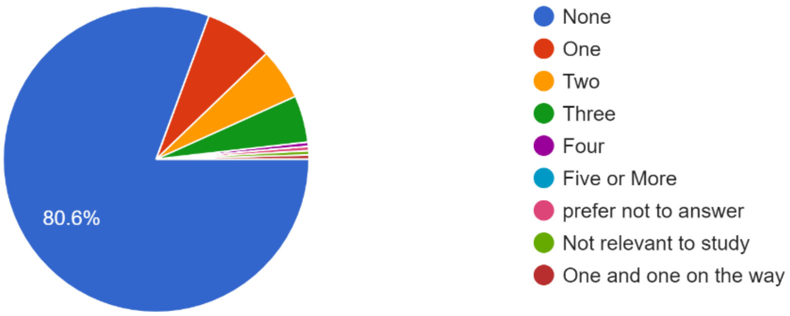
What is your highest level of education?

226 responses



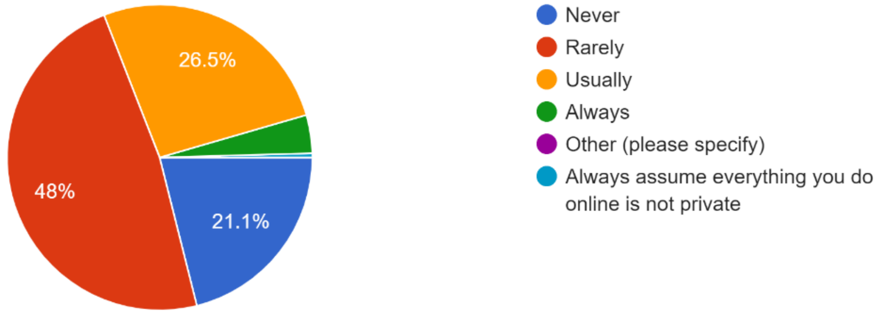
How many children do you have?

222 responses



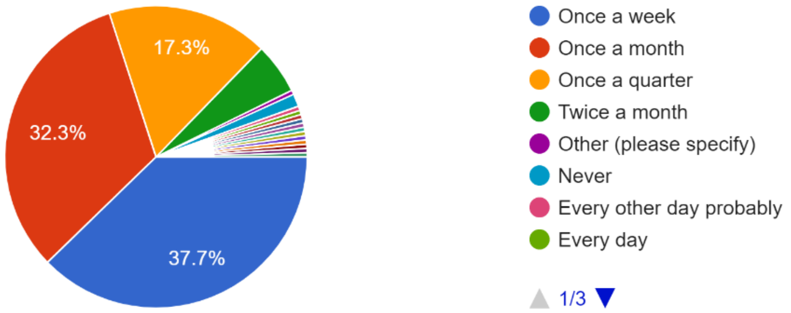
How often do you think your privacy is preserved while online over the internet?

223 responses



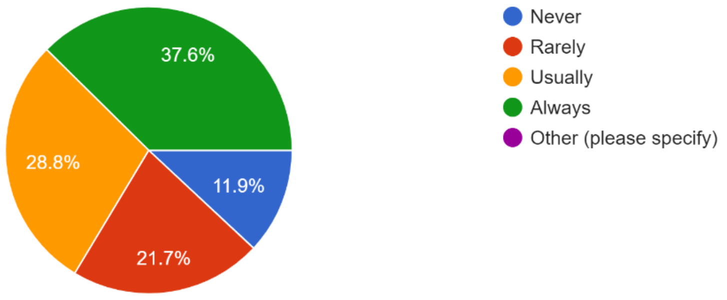
How often do you provide your personal information to access or use any application on the internet?

220 responses



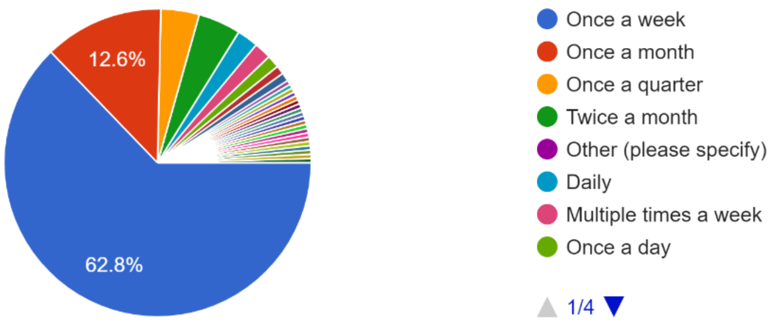
How often do you ensure and enforce security while using online applications over the internet by ensuring your firewall is set on and antivirus active?

226 responses



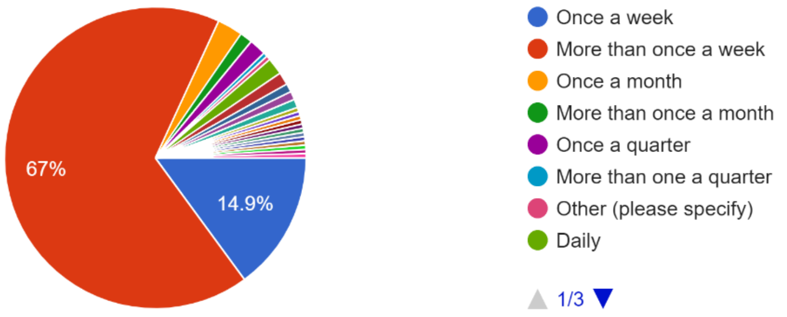
How often do you use your mobile device to access your banking apps?

223 responses



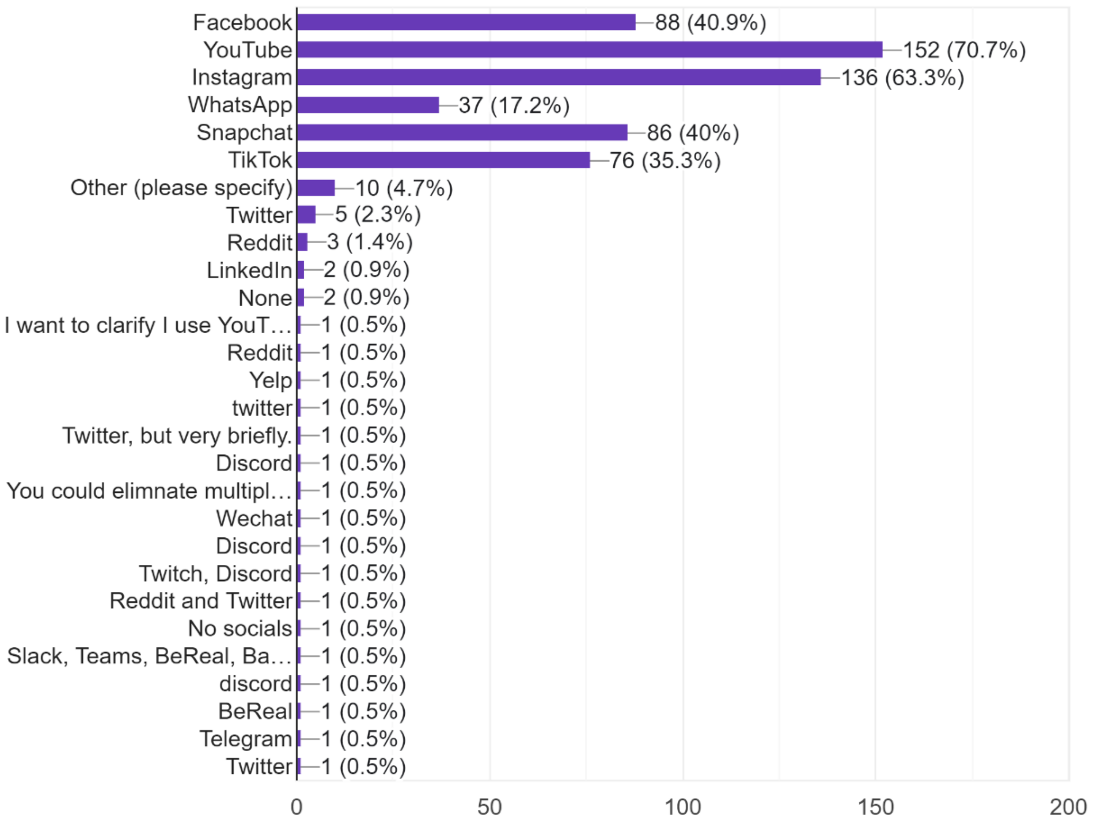
How often do you use your mobile device to access your social media apps?

221 responses



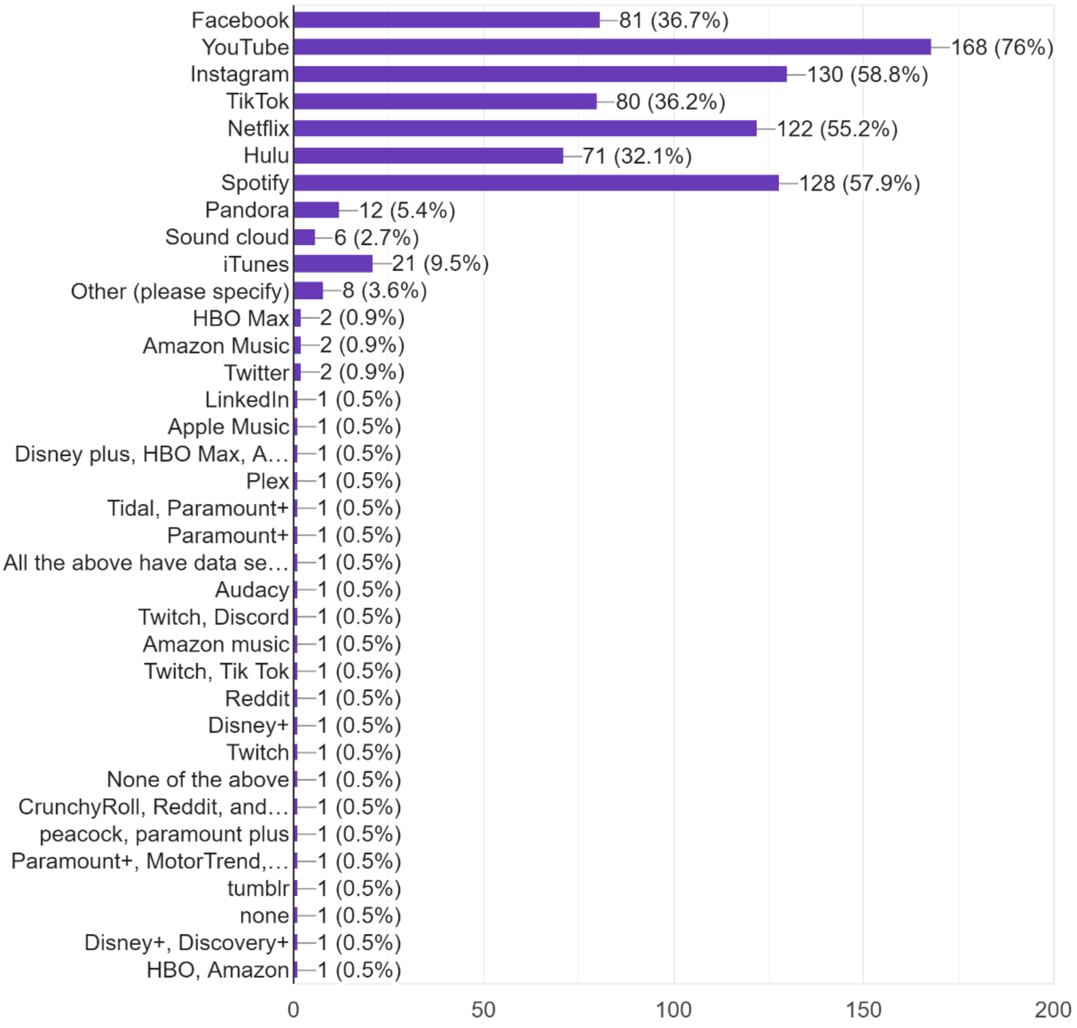
Which social media apps do you use more than five times a week? Select

215 responses



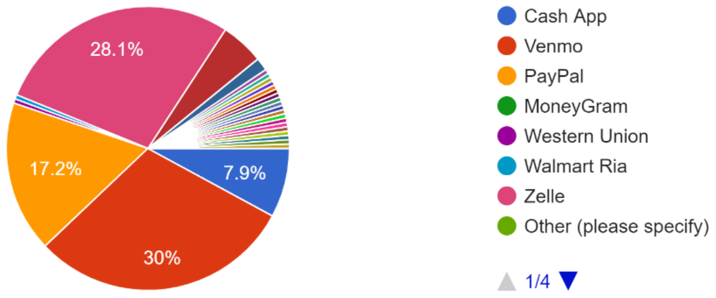
Which media streaming apps do you use more than three times a week?

221 responses



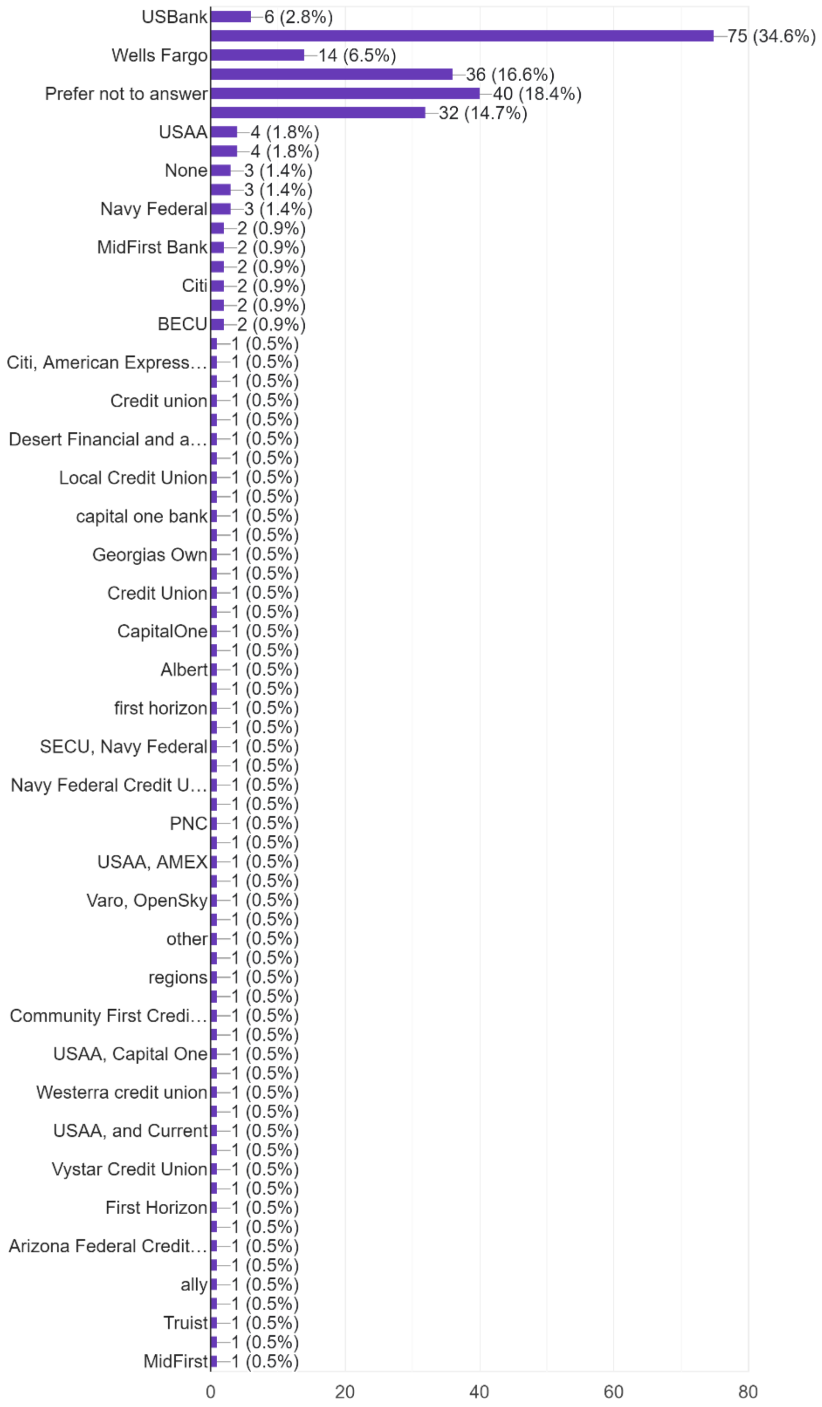
Which money transfer apps do you use more than once a month?

203 responses



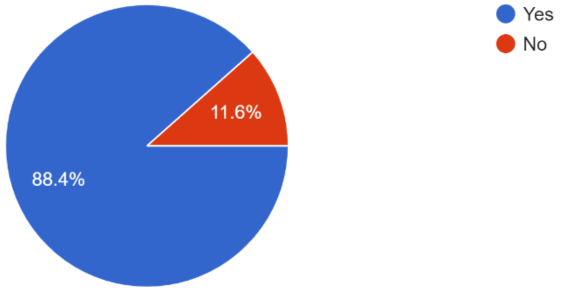
Which online banking apps do you often use?

217 responses



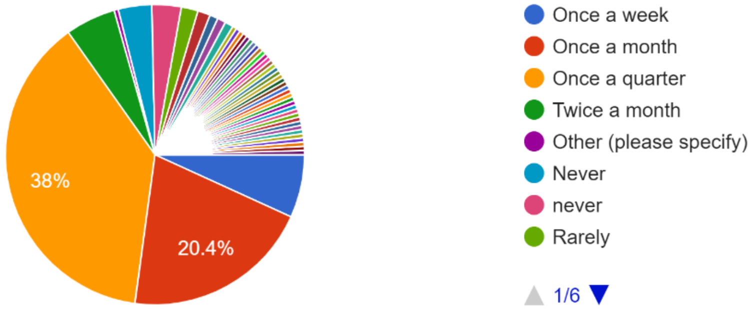
Do you use online banking apps more than your local bank branch or ATM for your banking needs?

225 responses



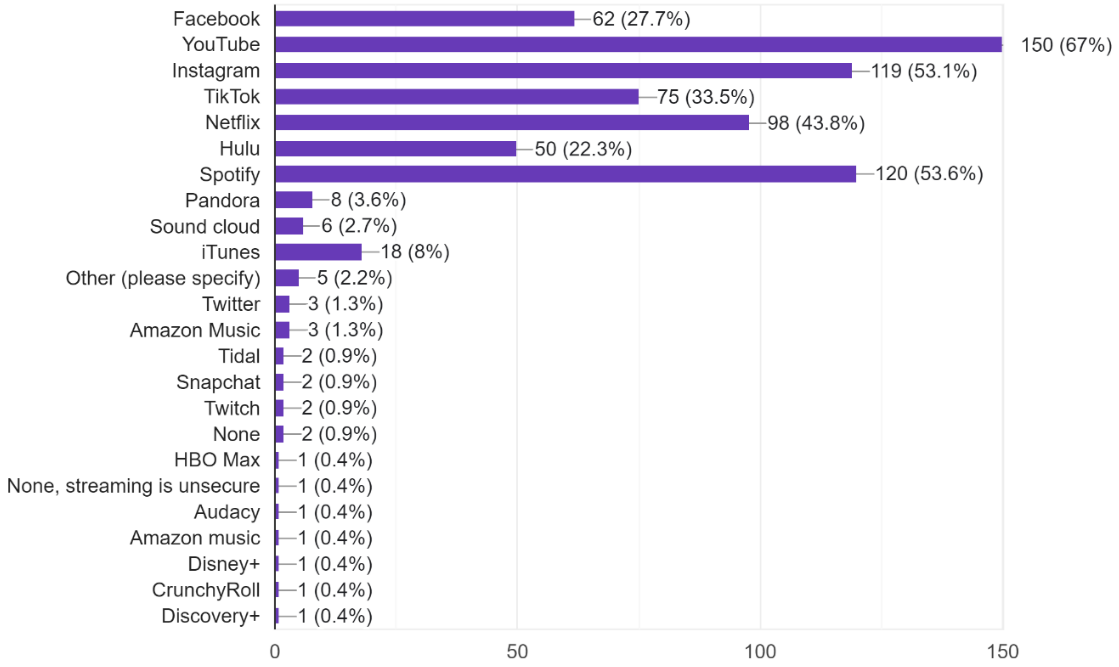
How often do you visit your local bank branch or ATM for your banking needs?

221 responses



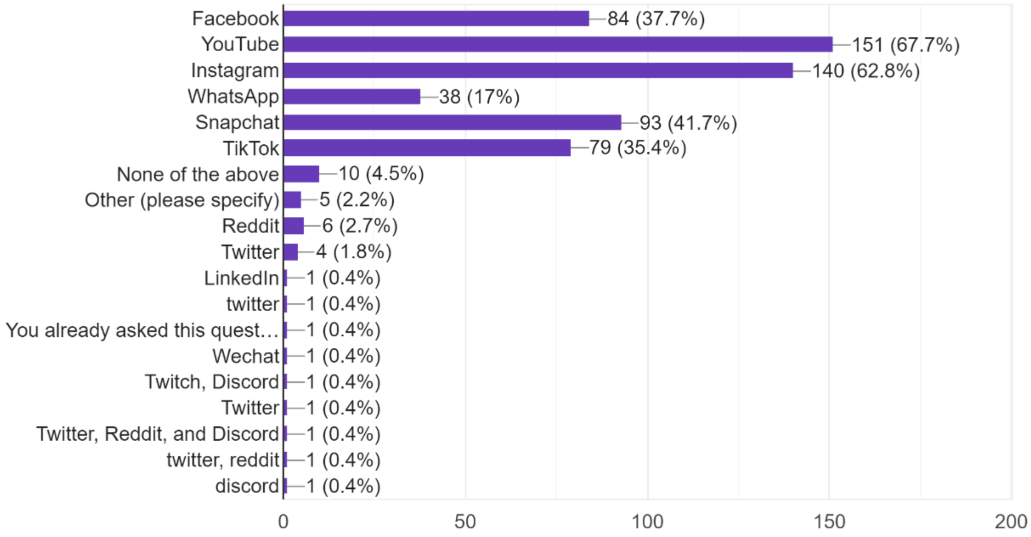
Which media streaming apps do you use more than 15 minutes a day?

224 responses



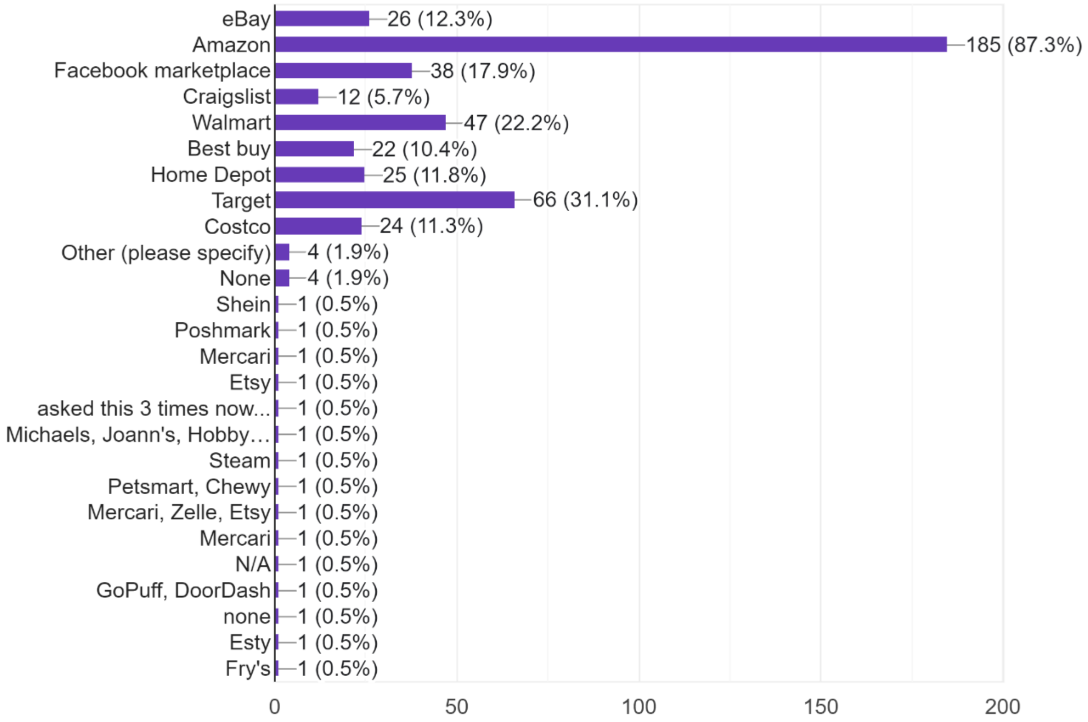
Which social media apps do you use more than once a day?

223 responses



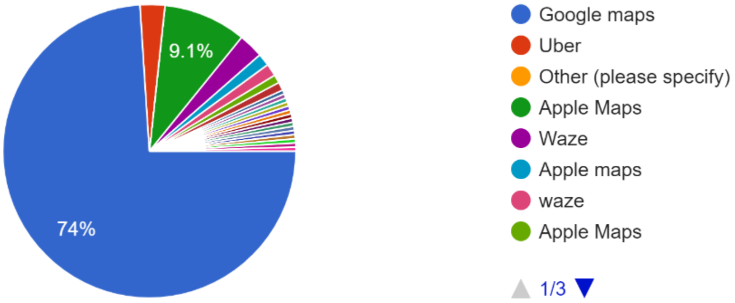
Which ecommerce apps do you use more than once a month?

212 responses



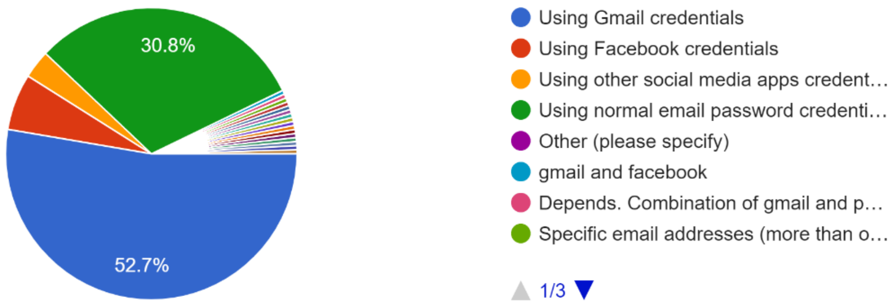
Which Location or direction apps do you use more than once a month?

219 responses



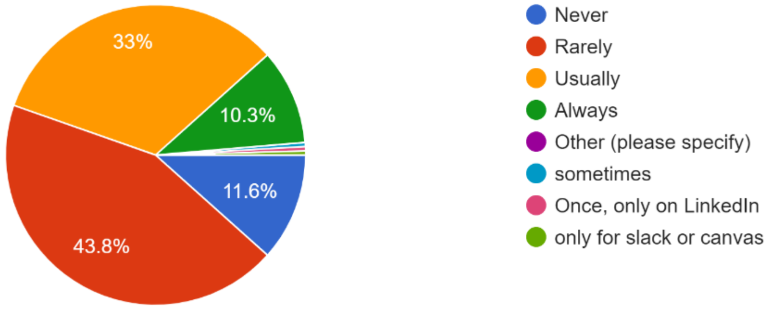
How do you sign into other apps?

224 responses



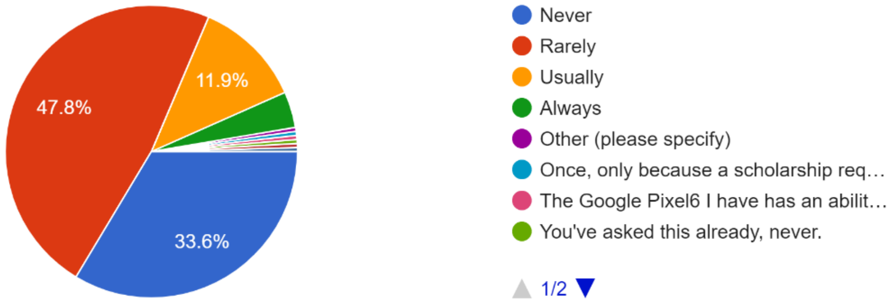
How often do you share your image or picture on social media/apps?

224 responses



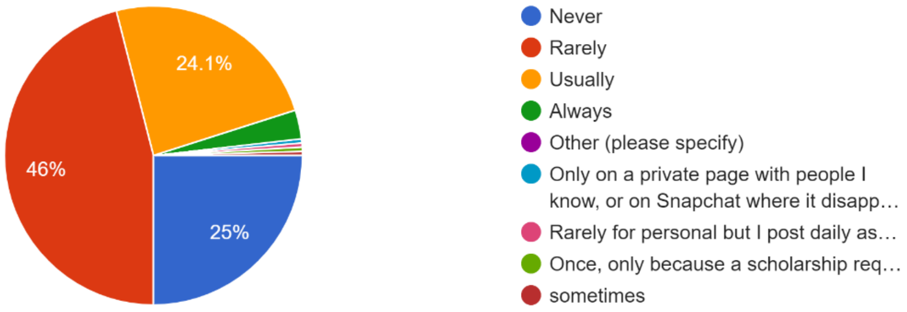
How often do you share your audio clips on social media/apps?

226 responses



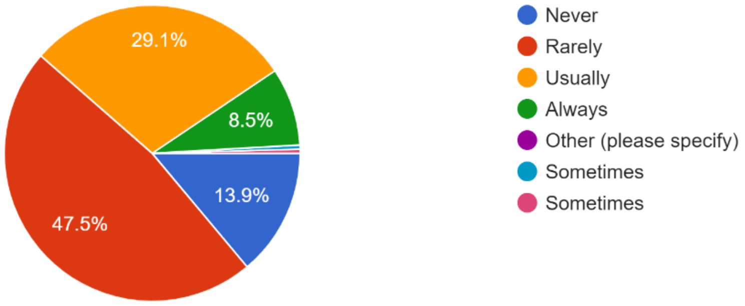
How often do you share your video clips on social media/apps?

224 responses



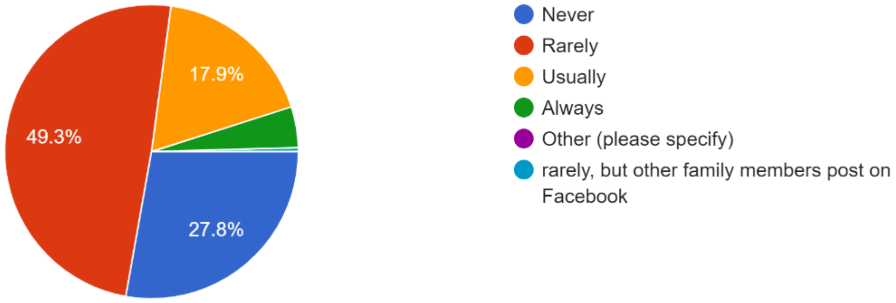
How often do you share images or pictures where you can be identified on social media/apps?

223 responses



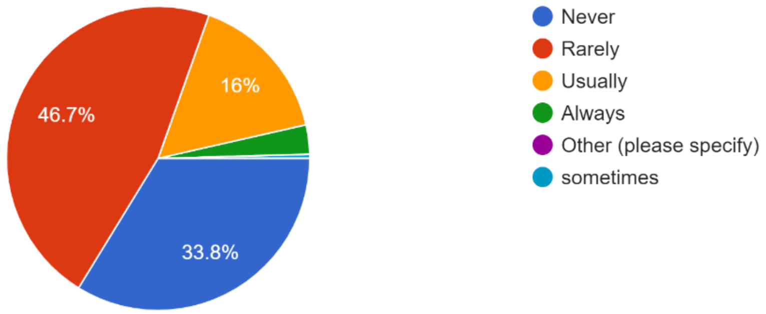
How often do you share videos where you can be identified or heard on social media/apps?

223 responses



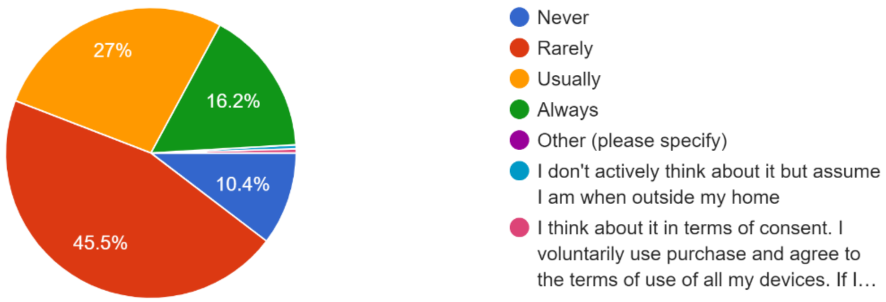
How often do you share audio clips where you can be heard on social media/apps?

225 responses



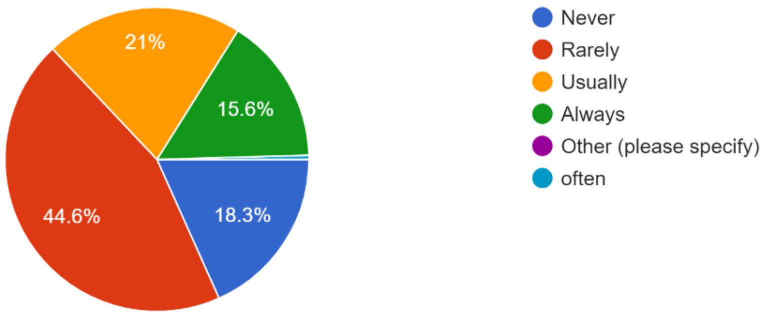
How often do you think about being recorded/on tape with or without your consent?

222 responses



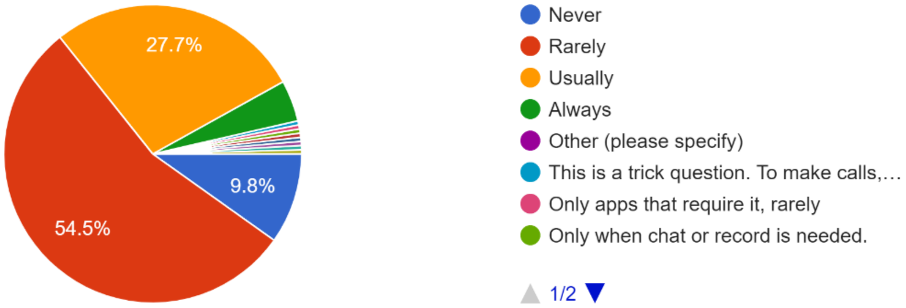
How often do you video chat or call on social media?

224 responses



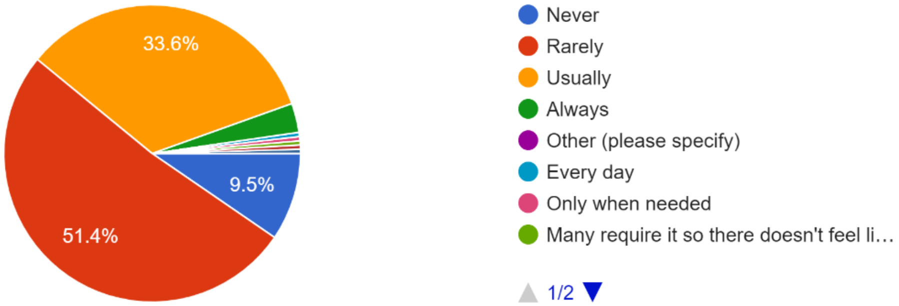
How often do you allow apps to access and control your mobile device microphone?

224 responses



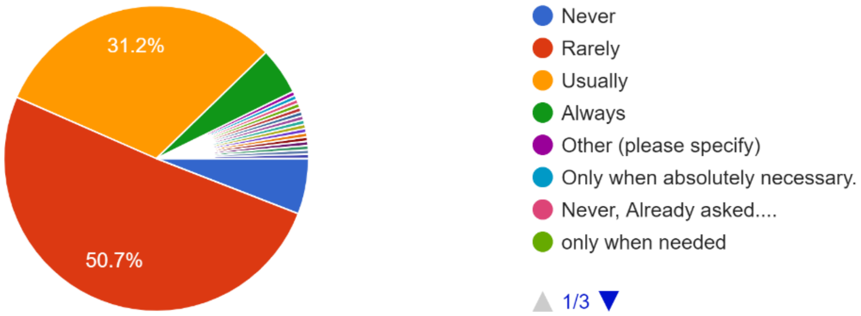
How often do you allow apps to access and control your mobile device camera?

220 responses



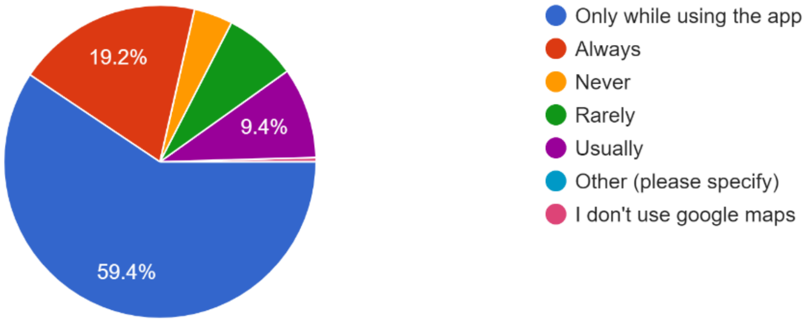
How often do you allow apps to access your mobile device location?

221 responses



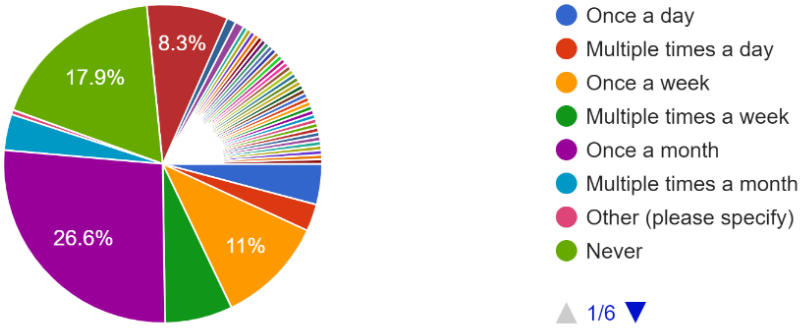
How often do you allow google maps to access your mobile device's current location?

224 responses



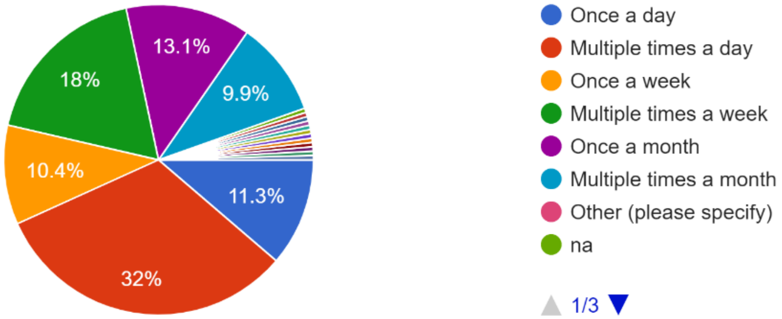
How often do you allow answer calls from unknown numbers?

218 responses



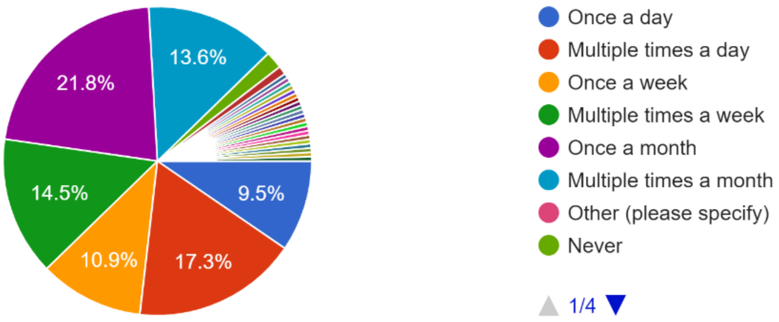
How often do you reject block phone calls from unknown numbers?

222 responses



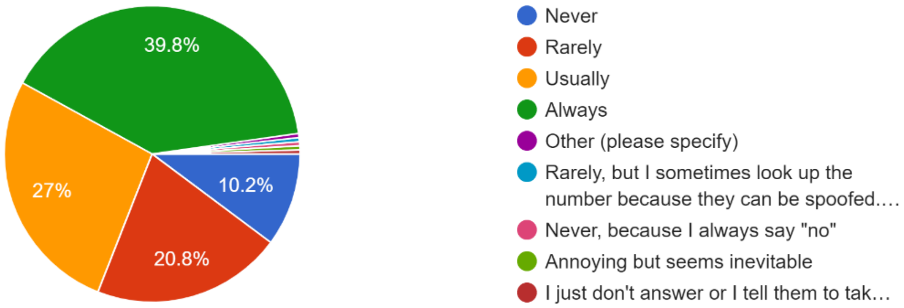
How often do you block unknown phone numbers?

220 responses



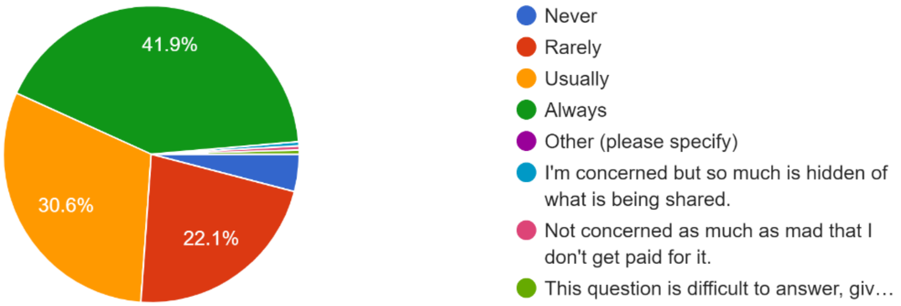
Do you have concerns when unknown numbers call you for solicitations?

226 responses



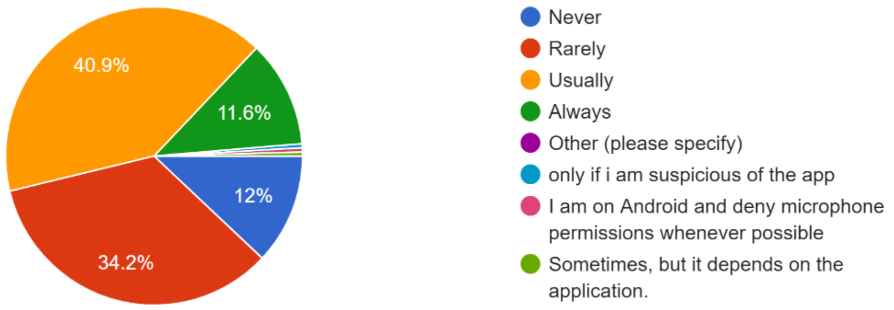
How concerned are you with your information being sold to third parties?

222 responses



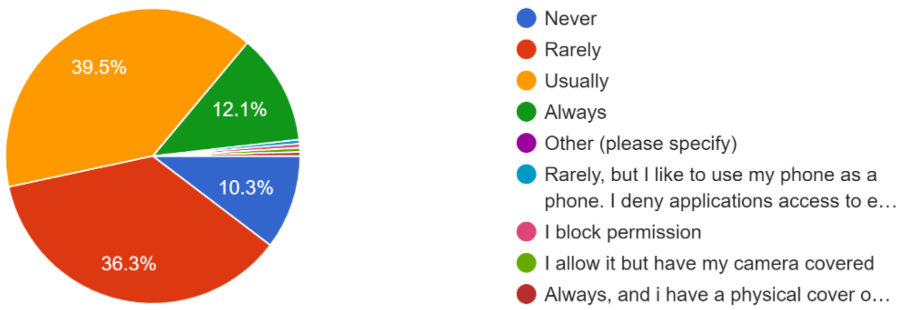
How often do you block or uninstall applications wanting to control your device's microphone?

225 responses



How often do you block or uninstall applications wanting to control your device's camera?

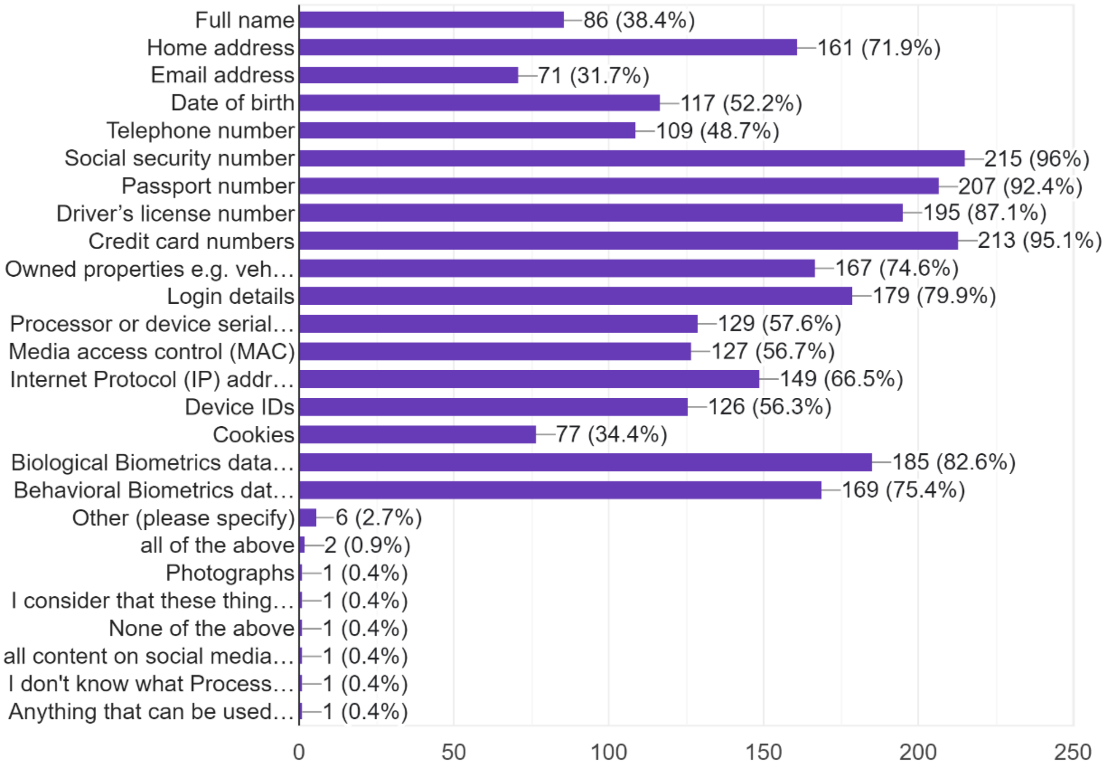
223 responses



,

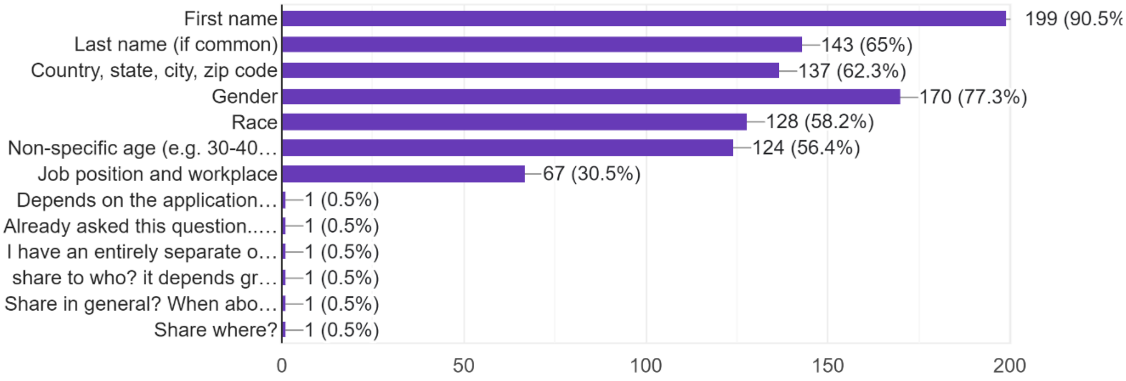
Which of the following information do you consider private?

224 responses



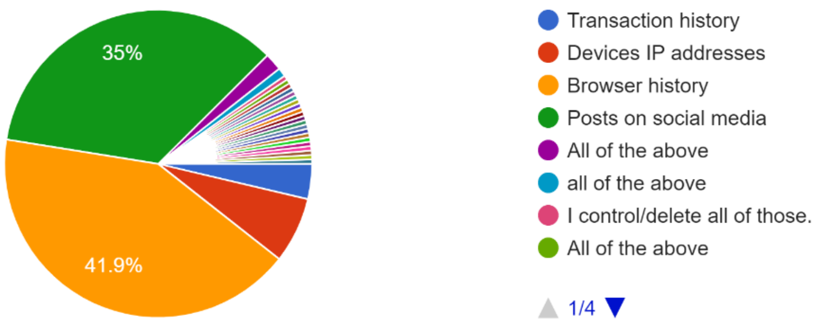
Which of the following do you share?

220 responses



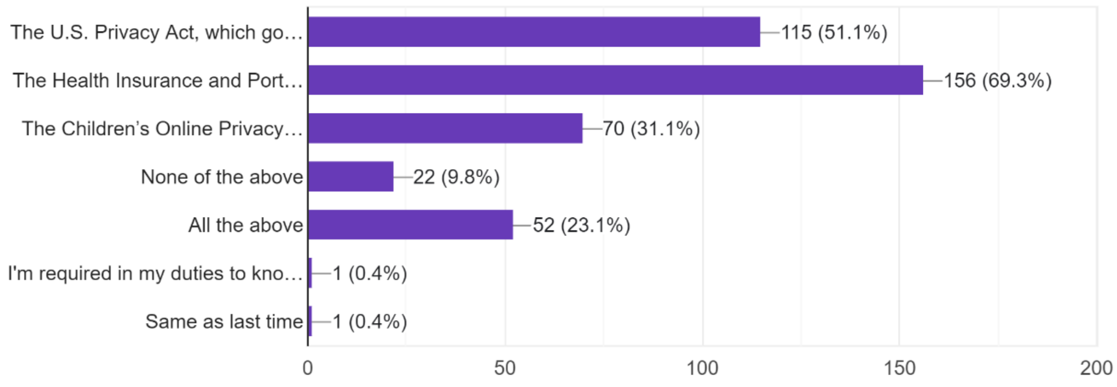
Which of the following do you share, control, or delete?

217 responses



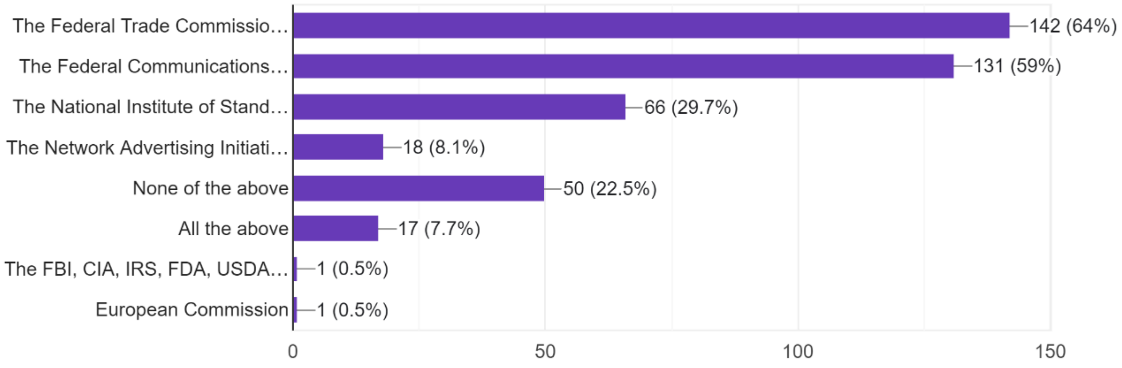
Which of the following frameworks or institutions do you know or heard of?

225 responses



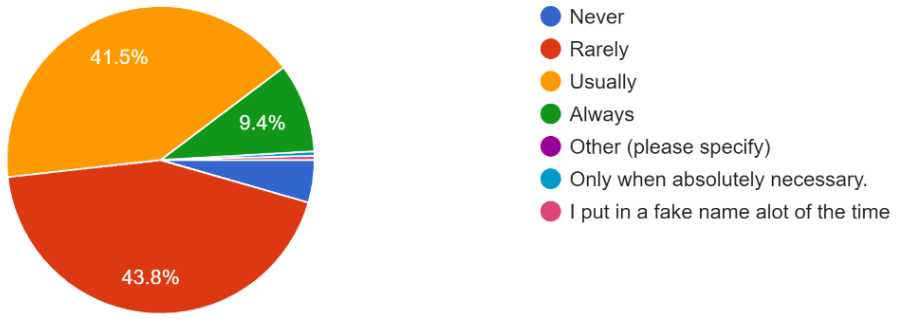
Which of the following organizations do you know?

222 responses



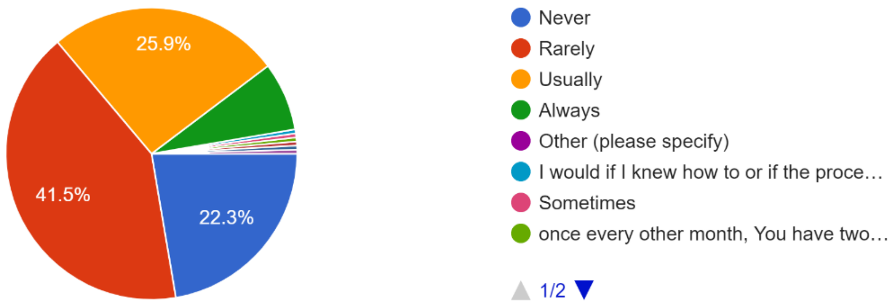
How often do you provide your full name information online, in apps or for services over the internet?

224 responses



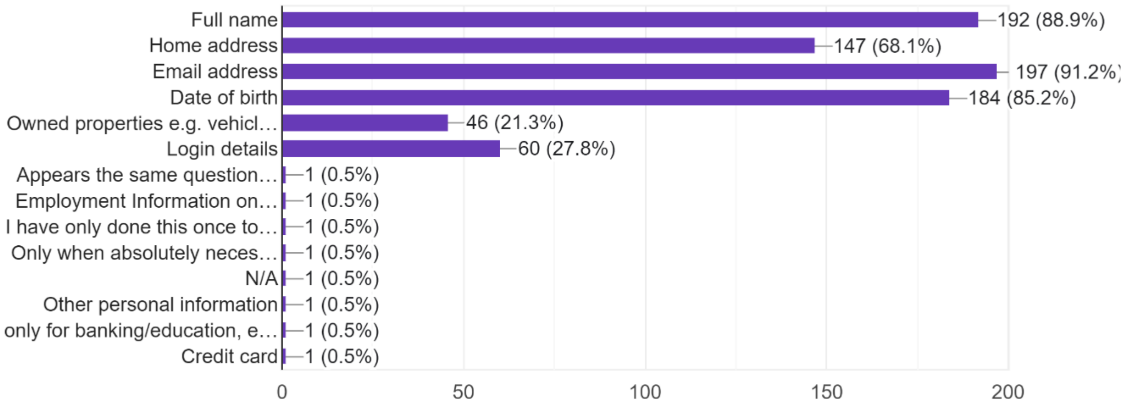
How often do you ask for your personal information to be deleted from online applications or from services applications over the internet?

224 responses



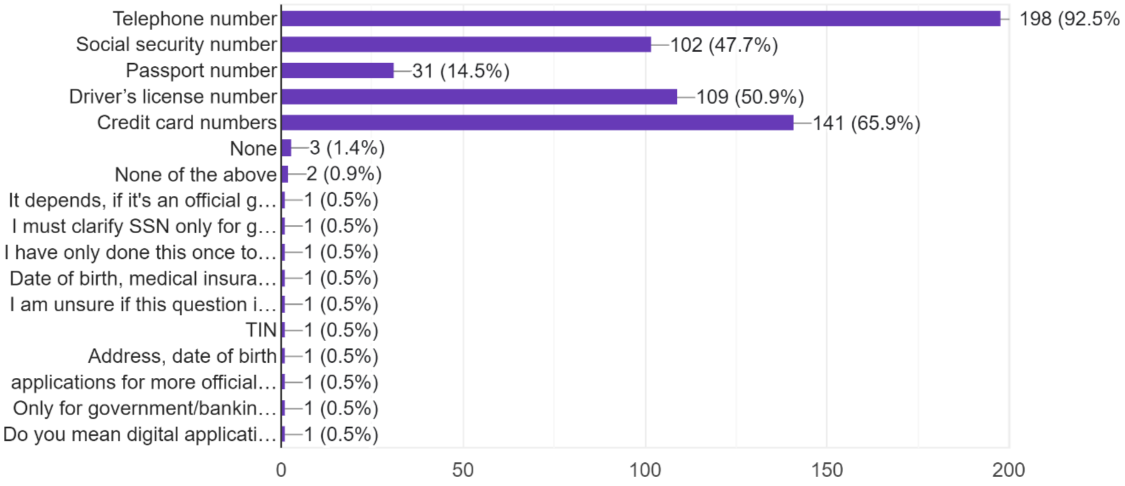
Which of the following information have you shared online or in applications?

216 responses



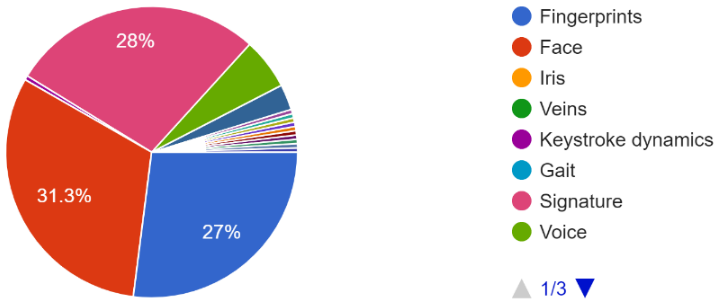
Which of the following information have you shared online or in applications?

214 responses



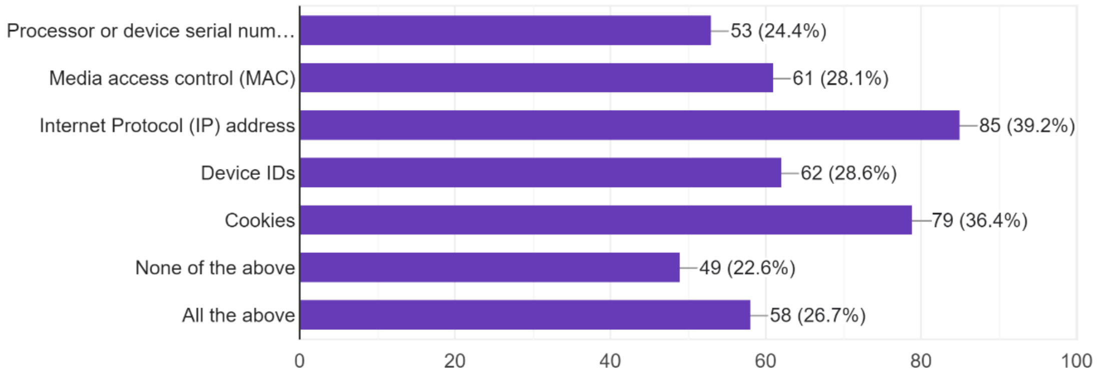
Which of the following information have you shared online or in applications? Biological Biometrics data (fingerprints, face, iris, veins, etc.) Behaviora...ta (keystroke dynamics, gait, signature, voice, etc.)

211 responses



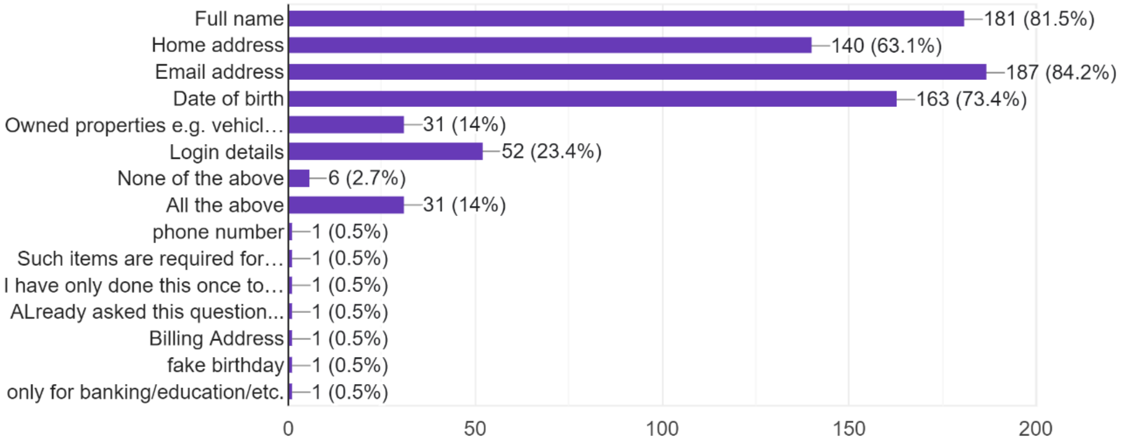
Which of the following information do you care about while online or using applications?

217 responses



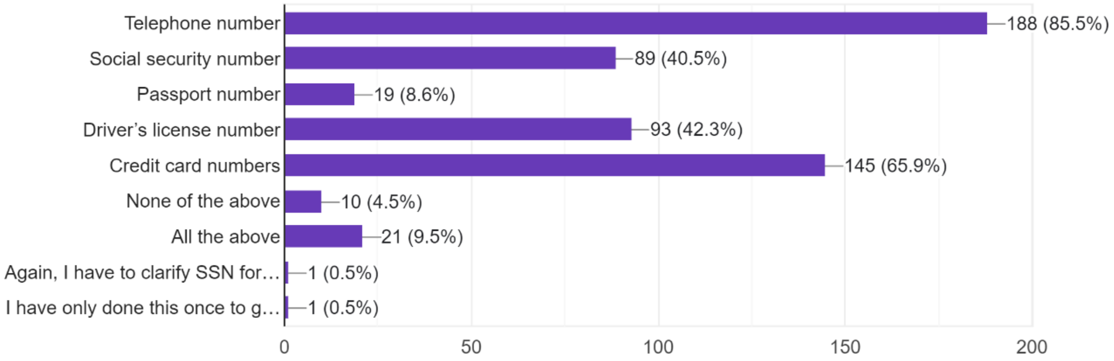
Which of the following information have you shared online for specific services over the internet?

222 responses



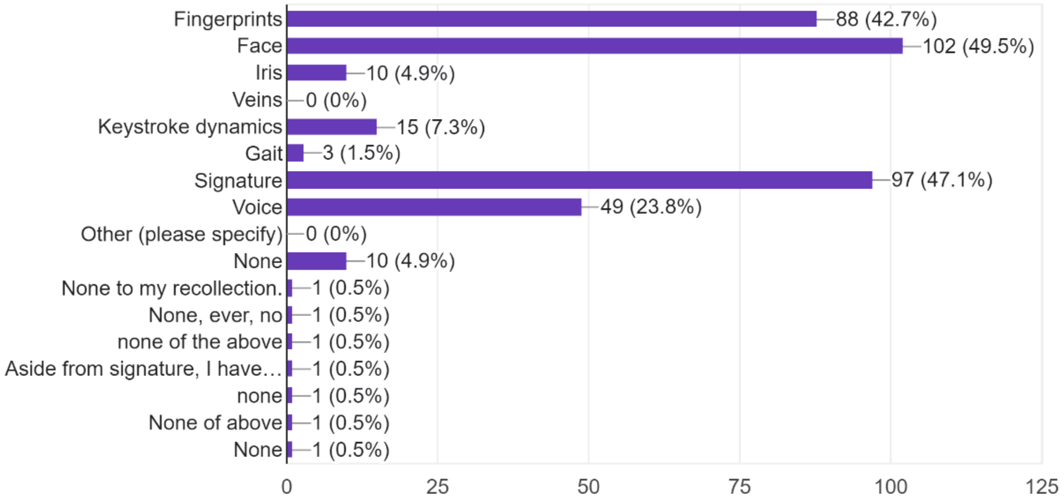
Which of the following information have you shared online for specific services over the internet?

220 responses



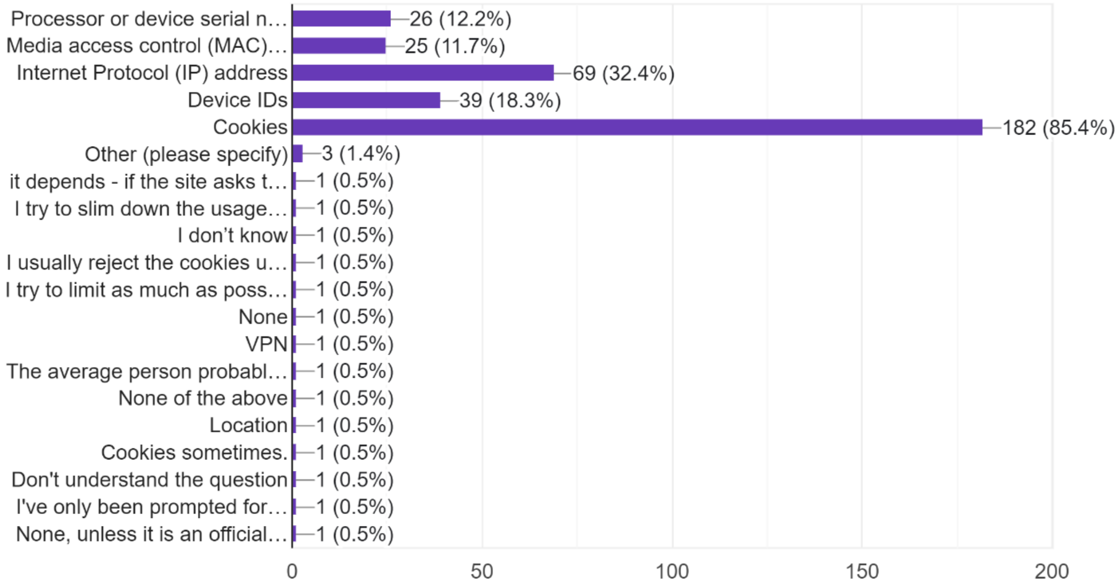
Which of the following Biometrics information have you shared online for specific services over the internet?

206 responses



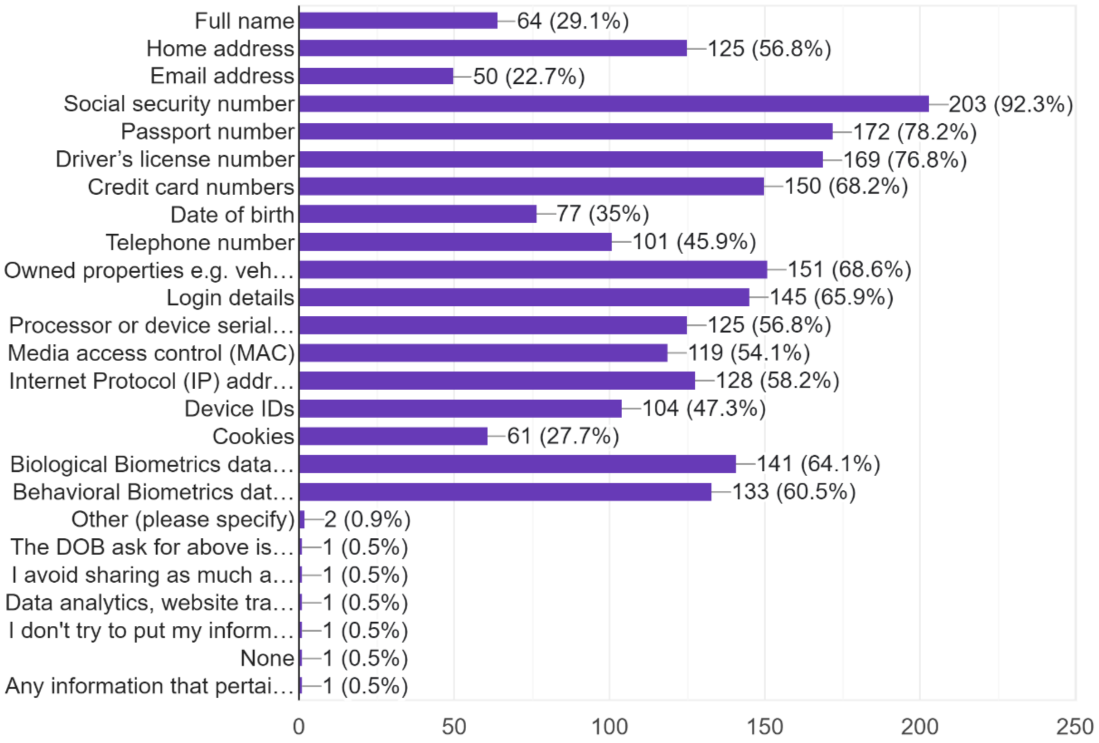
Which of the following information do you accept your browser to access online or over the internet when prompted?

213 responses



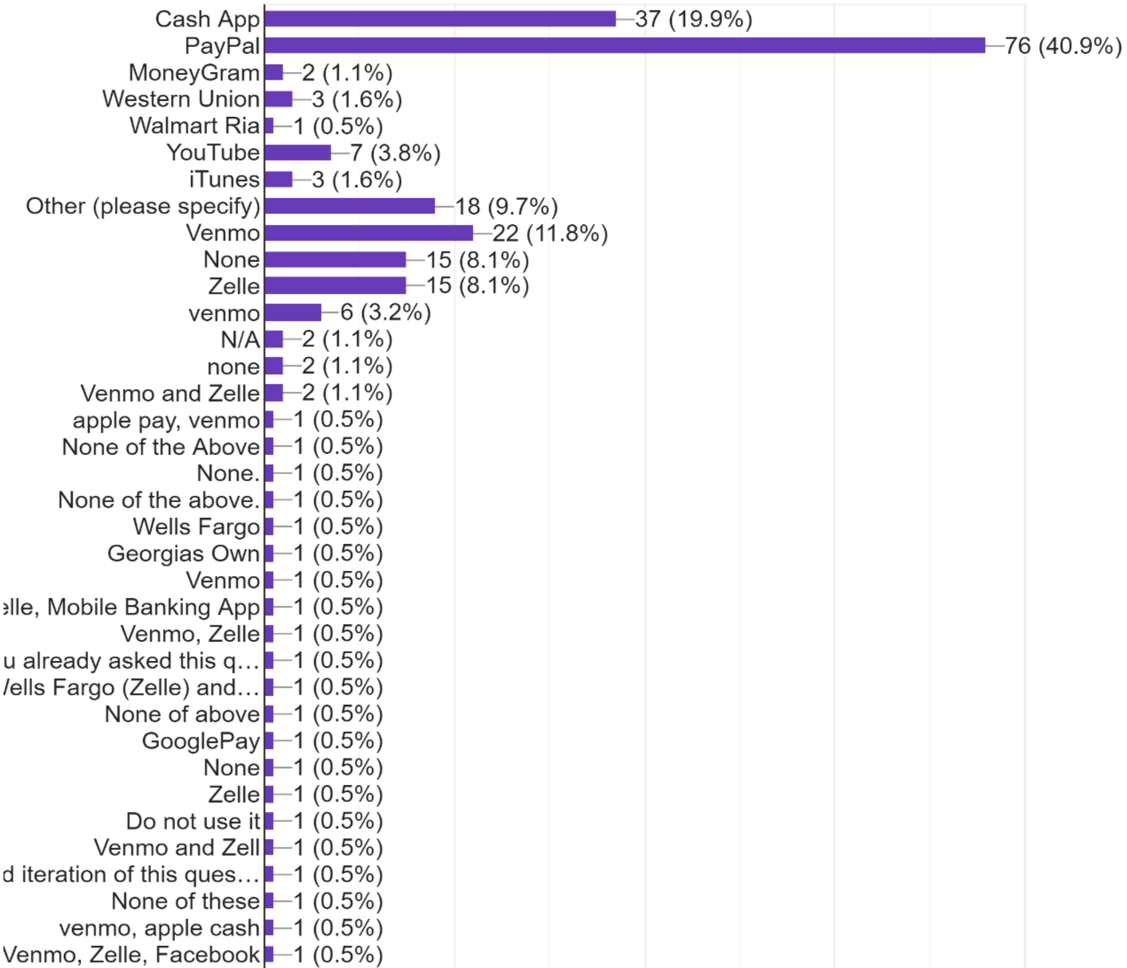
Which of the following information do you actively avoid sharing online?

220 responses



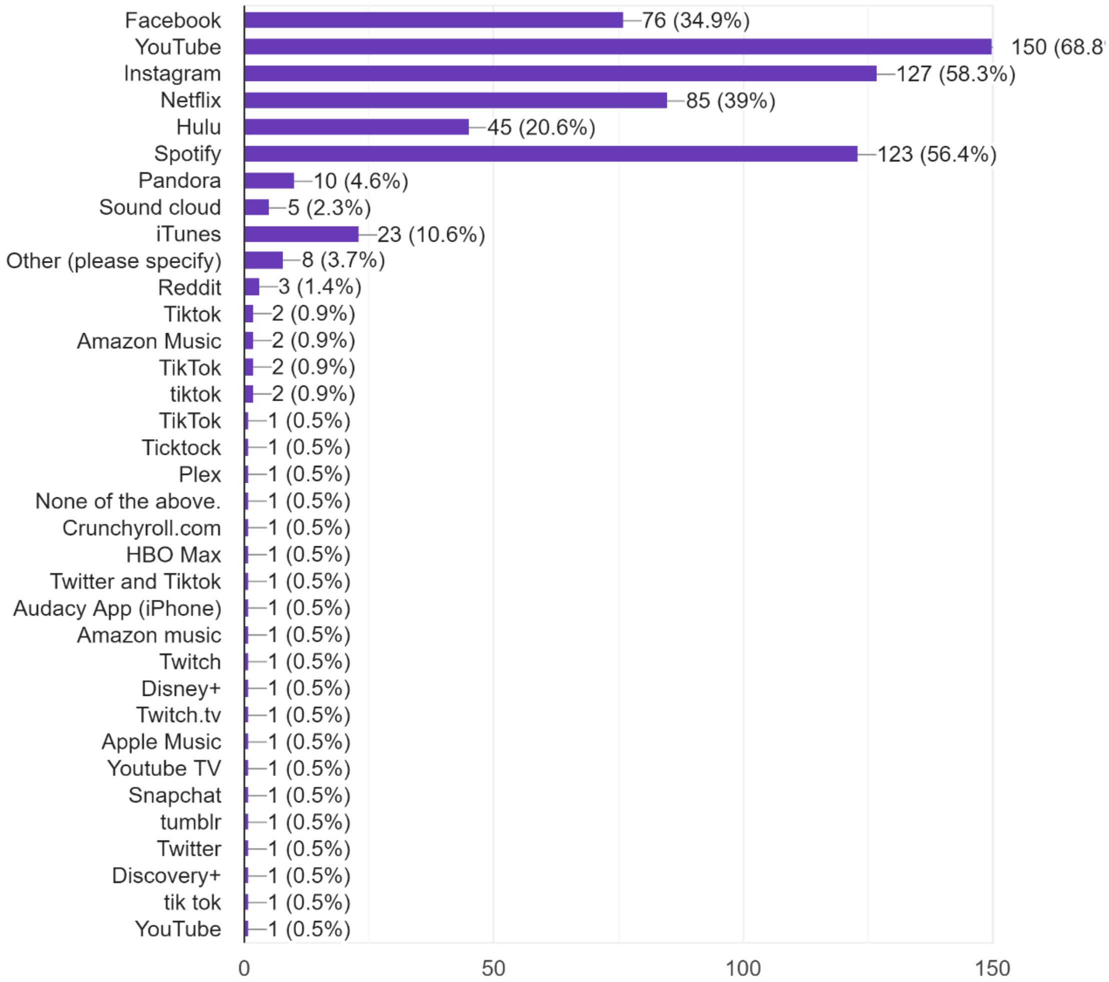
Which money transfer apps do you use more than once a month?

186 responses



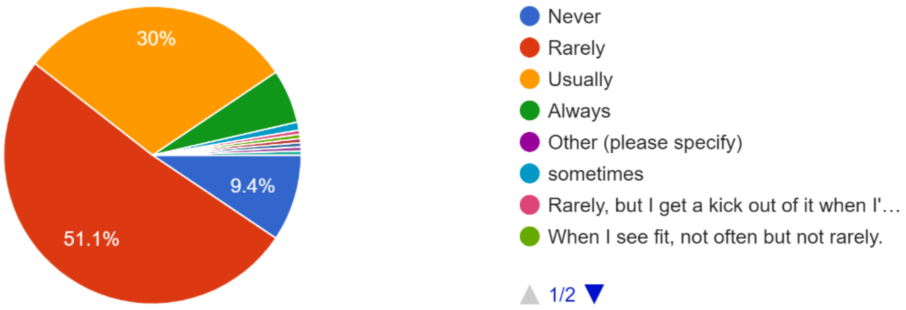
Which media streaming apps do you use more than once a day?

218 responses



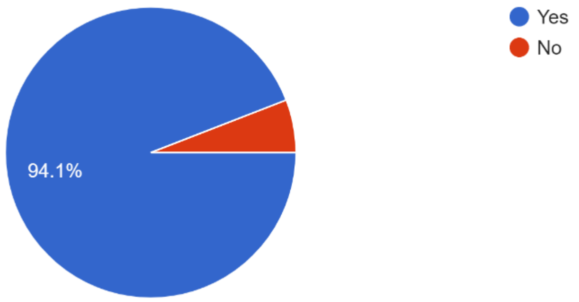
How often do you refuse to consent to software or online applications for services over the internet?

223 responses



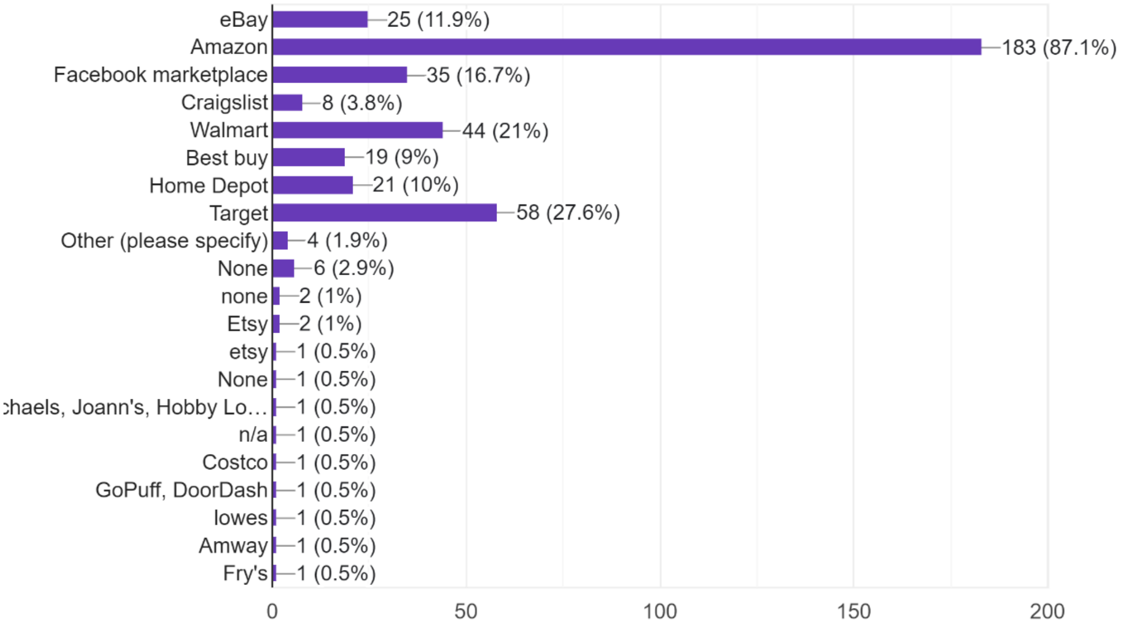
Would you wish to have an application that grants you control of your private information and notify you whenever your private information is bei... or requested in applications or over the internet?

221 responses



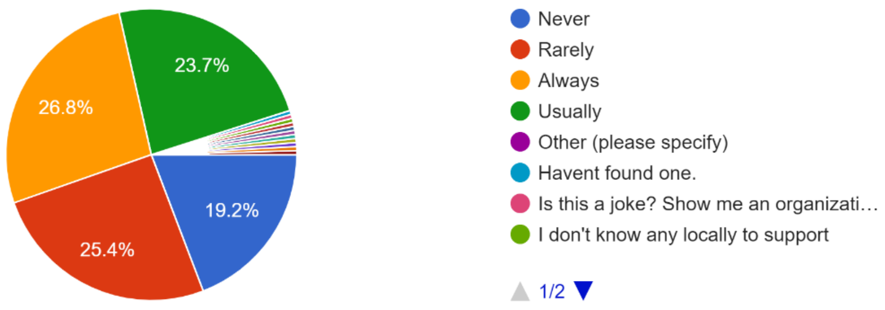
Which ecommerce apps do you use more than twice a month?

210 responses



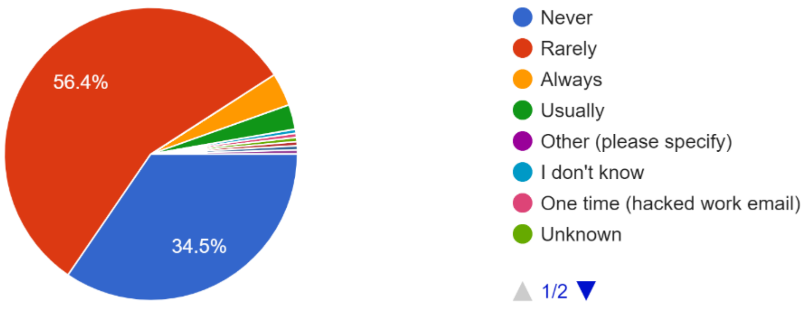
How often do you support organizations that aim to reinforce the preservation of citizen's privacy online?

224 responses



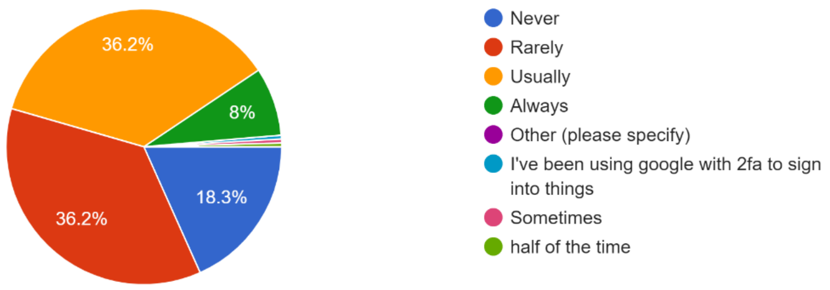
How often have you been affected by a potential cyber-attack in online applications and over the internet?

220 responses



How often do you sign into other apps using your social media credential?

224 responses


Never
Rarely
Usually
Always
Other (please specify)
I've been using google with 2fa to sign into things
Sometimes
half of the time