CERIAS Tech Report 2024-2

Exploring Factors Influencing Adoption and Usage of Privacy-Enhancing Tools Among Smartphone Users.

by Renusree Varma Mudduluru
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

EXPLORING FACTORS INFLUENCING ADOPTION AND USAGE OF PRIVACY-ENHANCING TOOLS AMONG SMARTPHONE USERS

by

Renusree Varma Mudduluru

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

August 2024

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Marcus K. Rogers, Co-Chair

Department of Computer and Information Technology

Dr. Tatiana R. Ringenberg, Co-Chair

Department of Computer and Information Technology

Dr. Smriti Bhatt

Department of Computer and Information Technology

Approved by:

Dr. Stephen J. Elliott

Dedicated to my family

ACKNOWLEDGMENTS

I want to express my heartfelt appreciation to my family for their steadfast support and encouragement. Their unwavering belief in me has been an invaluable source of motivation throughout my journey. Additionally, I am deeply grateful to my family and friends for their support, which has played a pivotal role in helping me reach this point.

I want to express my sincere gratitude to Dr. Marcus K. Rogers for his invaluable help during my thesis proposal and research study. I deeply appreciate the time and effort he invested in helping me achieve my goals. During critical junctures, his support in resolving challenges, whether in formulating research questions or during data analysis, proved invaluable. I am grateful for his unwavering support and guidance, which played a pivotal role in my project's success. I am immensely grateful for his readiness to respond to my questions, review my work, and provide valuable feedback, particularly given that this was my initial experience with a major thesis project. Once again, I express my deepest appreciation for all that Dr. Marcus K. Rogers has done for me.

I would like to extend my sincere gratitude to Dr. Tatiana R. Ringenberg for her invaluable guidance and support throughout my research journey on data analysis and formulating my survey questions. Her insights into MTurk, survey methodologies and applying IRB proved immensely beneficial in designing and conducting my quantitative survey. Furthermore, her willingness to answer my questions greatly aided in clarifying key aspects of the research process.

I would also like to express my deep appreciation to Dr. Smriti Bhatt for her invaluable contributions. Her insights into finalizing survey questions proved immensely beneficial in designing and conducting my quantitative survey. Furthermore, her willingness to answer my questions greatly aided in clarifying key aspects of the research process.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

ANOVA	Analysis of Variance formula
GPS	Global Positioning System
IRB	Institutional Review Board
Mturk	Mechanical Turk
OS	Operating System
PII	Personally Identifiable Information
SPF	Service Privacy Fit
VPN	Virtual Private Network

ABSTRACT

In this era of digital surveillance and data breaches, it is important to understand how users protect their smartphone privacy. There needs to be more detailed information regarding the prevalence, factors, and motivations influencing the adoption of privacy-enhancing tools and settings on mobile devices. This study aimed to address this knowledge gap by investigating the use of privacy tools among smartphone users and examining the impact of factors like demographics, awareness levels, and device platforms.

The study surveyed 342 participants recruited through Amazon Mechanical Turk (MTurk), and the data were analyzed. The survey gathered data on user characteristics, privacy concerns, experiences with breaches, and use of various privacy tools. Statistical analysis showed that demographic factors, particularly age, significantly influenced the use of privacy tools, aligning with previous research. Users with a higher awareness of digital privacy risks were likelier to adopt privacy-enhancing tools. The study found no significant difference in the prevalence and type of privacy tools used between iOS and Android users.

The study's focus on privacy-enhancing tools among smartphone users and the proposed hypotheses provide valuable insights for law enforcement and forensic practitioners, aiding in digital investigations, evidence collection, and understanding user behavior related to smartphone privacy measures. The study's outcomes contribute to digital forensics, cybersecurity, and privacy domains by providing insights into user behaviors, motivations, and the factors shaping privacy tool adoption on smartphones. These findings can inform the development of more user-centric privacy tools, policies, and educational campaigns, ultimately enhancing digital privacy protection and supporting law enforcement investigations in the digital age.

1. INTRODUCTION

This chapter's primary emphasis revolves around examining the study, research questions, and the problem statement. Additionally, it provides an extensive account of the limitations, delimitations, and assumptions.

1.1 Background

In the digital age, privacy is important, especially with smartphones, because of the immense amount of personal information they gather. According to Zou et al. (2020), these devices have robust computational powers and sensors that can monitor various user actions and attributes. Due to the possibility of misuse or compromise, the massive data collection poses serious privacy concerns (Ayres-Pereira et al., 2022). There are plenty of possible threats connected to the data that smartphones collect. Smartphones contain various sensitive data that, if exposed, can result in privacy breaches and even physical threats. Examples include tracking user's locations through GPS data (Mosenia et al., 2018) and assessing personality traits based on app usage (Chittaranjan et al., 2011). Users must know the risks of sharing personal data through smartphones and the potential consequences of data breaches (Yan et al., 2019).

Smartphones are becoming essential tools for privacy analysis because of the sensors and functionalities they contain, particularly in contact-tracing apps (Azad et al., 2021). Smartphone privacy-enhancing tools include many technologies that protect user information such as VPNs, password managers, app permissions, encryption, antivirus software, and default settings. Recent studies on usable privacy research state that technological solutions like access control and authentication, and new techniques like homomorphic encryption and differential privacy demonstrate the rapid growth of privacy-enhancing technologies (Tahaei et al., 2022). Perceived risks and desired protection levels impact user's willingness to interact with privacy-protecting tools (Meier et al., 2021). Addressing security concerns and improving privacy regulations are still crucial as smartphones are rapidly used in industries like healthcare and education (Jabali et al., 2019). Smartphone privacy-enhancing tools are continuously evolving, requiring further studies to ensure the security and privacy of user data. Though privacy-enhancing tools are available, user-related challenges still exist (Meier et al., 2021). The development of smartphone privacy-

protecting tools should consider user preferences and the context dependency of their decisions (Wettlaufer & Simo, 2020; Carelli et al., 2019). Studies have emphasized the importance of user-centric privacy approaches, customizing privacy practices to individual preferences to boost user engagement with privacy-enhancing technologies (Knijnenburg et al., 2021). Understanding the usability of smartphone manufacturers' default features and privacy settings is essential in promoting user awareness and control over their data (Ramokapane et al., 2019). Maseeh (2023) highlighted the importance of understanding how people use smartphone privacy-enhancing features and settings. It emphasizes the significance of privacy concerns and their impact on users' behavioral intentions in the context of smartphone applications.

The increasing prevalence of smartphones in all age groups has highlighted the need to understand how users behave toward the application's privacy policies (Ullah et al., 2022). It is important to explore user's expectations and privacy concerns, especially when designing smartphone privacy management tools (Carelli et al., 2019). The study by Utz et al., (2021) has explored the importance of understanding the prevalence of privacy tool usage among smartphone users. This research shows how demographic factors, awareness levels, and smartphone platforms influence the adoption of privacy measures. It highlights the critical knowledge gap that hinders the development of effective privacy tools and policies, particularly relevant for digital forensics professionals (Utz et al., 2021)

1.2 Problem Statement

Understanding how people protect their digital privacy on smartphones in the era of increased digital surveillance and data leaks is important. Though there is an increase in digital privacy concerns, there needs to be more detailed information available about how, why, and how much people use privacy-enhancing apps and settings on their devices. This information gap makes developing effective privacy solutions, policies, and awareness campaigns difficult. The present study aimed to learn about the frequency of privacy tool usage and the factors that impact its usage among smartphone users. Specifically, the research focused on the impact of smartphone platforms, demographic characteristics, and awareness levels on adopting privacy measures. This lack of understanding makes it more difficult to create privacy policies and technologies useful to those operating in digital forensics. Addressing this research problem will contribute significantly

to digital forensics, cybersecurity, and privacy. It will help create more user-centric privacy tools and policies and educate users about the importance of digital privacy.

1.3 Research Question

The research questions for this study are:

1. How prevalent is the use of privacy-enhancing tools and settings among smartphone users?
2. What factors influence users' adoption and usage of privacy-enhancing tools?

1.4 Hypotheses

The hypotheses for this study are stated as:

1. There is a significant difference in the use of privacy tools among smartphone users based on demographic factors such as age and familiarity with cybersecurity.
2. Smartphone users with a higher awareness of digital privacy risks are likelier to use privacy-enhancing tools and settings on their devices.
3. The prevalence and type of privacy tools used differ significantly between iOS and Android smartphone users.

1.5 Assumptions

The study operates on the following assumptions:

1. It is assumed that the respondents will provide honest and accurate responses to the survey questions.
2. The research assumes that respondents have a basic understanding of privacy tools.
3. The research assumes that all respondents have equal access to privacy tools.
4. The data collected through self-reported responses are assumed to be valid and accurately represent participants' behaviors and attitudes toward smartphone privacy.

1.6 Limitations

The limitations of the study include:

1. The data collected is self-reported, which may introduce bias as respondents might overstate or understate their use of privacy tools.
2. The use of Mechanical Turk (MTurk) for data collection may introduce sampling bias as the demographics of MTurk users may not represent the general population.
3. Findings from the survey may have limited generalizability beyond the specific population surveyed, mainly if the sample size is small or needs to be more diverse.
4. The research is based on cross-sectional data, which provides a snapshot at a particular point in time. It does not capture changes in behavior over time. Also, while the survey aims to investigate differences between iOS and Android users, it may overlook differences within each platform or need to capture users who use multiple platforms.

1.7 Delimitations

The delimitations of the study include:

1. The study is delimited to smartphone users and does not consider users of other digital devices.
2. The survey defines privacy tools based on specific examples, potentially excluding other tools or practices that users employ to enhance their privacy on smartphones.
3. The survey primarily uses quantitative methods, limiting the depth of understanding compared to qualitative approaches that delve into the nuances of individual experiences and perspectives.

1.8 Summary

This research addresses the knowledge gap about the prevalence and factors affecting smartphone users' use of privacy-enhancing apps. This research aims to contribute to the domains of digital forensics, cybersecurity, and privacy by examining the impact of demographics, awareness levels, and smartphone platforms on privacy tool usage. The results will help develop more user-centric privacy laws and educate users about the importance of digital privacy. Despite the limitations of self-reported data and potential sampling bias, this

study serves as a foundation for future research and the development of effective privacy tools and policies.

2. LITERATURE REVIEW

The chapter offers a comprehensive analysis of the privacy and security adopted in smartphones by users.

2.1 Overview of Digital Privacy in the Smartphone Era

The increase in the use of smartphones in different fields has raised serious concerns about digital privacy in the smartphone era. Significant privacy challenges have been raised by the growing use of smartphones and mobile applications that are being used (Zhang et al., 2017). Though most smartphone users are aware of the possible risks of disclosing personal information on these devices, users often prioritize efficiency over privacy concerns when using smartphones (Tran et al., 2014). Research indicates people's decision to buy smartphones might be influenced by concerns about security and privacy (Belkhamza et al., 2019). The extensive collection of personal data through smartphones for various applications, including voice analysis in mental health, raised privacy, security, and legal concerns (Faurholt-Jepsen et al., 2016).

Due to the extensive use of smartphones and the significant amount of personal data they collect, privacy is essential in the smartphone era. Strong security measures for privacy are important because of the increasing smartphone usage in almost every field, including communication, healthcare monitoring, and financial transactions (Chatterjee et al., 2021). Studies have indicated that consumer's inclination to use mobile applications and platforms is greatly impacted by their level of trust in the security and privacy of their smartphones. This highlights the importance of privacy in building user confidence and guaranteeing continuous usage (Chin et al., 2012). Privacy problems need to be addressed as smartphones advance into our daily lives to safeguard users' sensitive information and keep them safe when using smartphone technology (Chatterjee et al., 2021). Concerns regarding data security and privacy have emerged among smartphone users due to increased digital health apps and the gathering of consumer digital data. Research shows that people are more aware of the dangers of disclosing private health information via smartphone apps, emphasizing privacy protection in the digital health space (Grande et al., 2021). Further, the COVID-19 pandemic has accelerated the use of digital tools for contact tracing and health monitoring, requiring a careful balancing act between public health advantages and

individual privacy rights (Gerdon et al., 2021). To build privacy-enhancing solutions that meet user's expectations and desires, it is essential to comprehend user views of health data privacy and consumer behavior toward digital health applications (Grande et al., 2021).

User's acceptance of mobile applications and services is influenced by the interplay between privacy concerns and personalization in the context of ubiquitous commerce. Studies have examined the impact of personalization features on users' views of privacy and inclinations to embrace mobile commerce applications. These findings highlight the necessity for businesses to handle privacy concerns along with personalized services (Sheng et al., 2008). Asserting the importance of privacy considerations in the design and implementation of digital services, it is important to find a balance between the benefits of personalization and user's privacy expectations to promote trust and acceptance of mobile commerce applications (Sheng et al., 2008). In the age of smartphones, maintaining data security, building user confidence, and promoting responsible smartphone usage across different areas depend on understanding the importance of privacy (Chin et al., 2012).

2.2 Evolution of Privacy-enhancing tools

The development of tools that enhance privacy has evolved with a focus on addressing concerns and behaviors related to smartphone usage. Research has shown the importance of understanding how people use smartphones and their attitudes towards privacy when considering these tools (Ohme et al., 2020). The balance between utilizing data for digital mental health tools and protecting user privacy highlights the complex nature of privacy issues in smartphone apps, which can impact user's decisions to use privacy enhancing tools (Torous & Haim 2018). Studying how features that protect privacy affect users' confidence and concerns can offer insights into why people continue using these smartphone tools (Zhou et al., 2021). As digital privacy evolves in the smartphone era, it is crucial to understand privacy concerns and user behaviors. Research on how risks and privacy influence seniors' intentions to use smart healthcare services emphasizes the importance of considering privacy when adopting digital tools (Yen, 2022). Examining how people view privacy at their age and their perceptions, researchers can gain valuable insights into the complex nature of privacy and its impact on smartphone users' adoption of tools that enhance privacy (Kovanič & Spáč 2022).

The rise of smartphone applications in healthcare emphasizes the importance of implementing strong privacy measures to safeguard sensitive medical data (Mosa et al., 2012). Furthermore, the use of smartphones for tasks such as contact tracing during events like the COVID-19 pandemic underscores the significance of tools that enhance privacy to ensure data security while using these technologies for health purposes (Benthall et al., 2022). With smartphones serving as hubs for numerous services and data operations, the necessity for effective tools that enhance privacy to uphold user confidentiality and data protection becomes crucial (Benthall et al., 2022). As smartphone users navigate through default settings and apps, a growing demand exists to empower them with tools that provide visibility and control over their privacy settings (Carelli et al., 2019).

Context-aware techniques leverage smartphone sensors like GPS, accelerometers, and microphones to infer and utilize users' contexts, enabling personalized services such as location-based reminders and activity tracking. Early approaches suppressed sensitive contexts while releasing non-sensitive ones, but this was vulnerable to adversaries inferring the sensitive data using temporal correlations between contexts and new approaches like MaskIt improved on this by also suppressing some non-sensitive contexts to reduce those temporal correlations. Through these methods, like context-aware techniques for preserving privacy, users can effectively manage their preferences regarding privacy while using smartphones (Zhang et al., 2017).

Privacy enhancing tools play a role in securing personal information on smartphones. Encryption applications, VPNs, ad blockers, password managers, and various other technologies are now commonly used by smartphone users to safeguard their data (Sharma, 2020). VPN apps establish encrypted connections for internet traffic, ensuring the protection of all data transmitted and received (Alashi & Aldahawi 2020). Ad blockers assist users in avoiding tracking and targeted ads, thereby boosting online privacy (Sharma, 2020). Password managers securely handle complex passwords to lower the risk of unauthorized access to important accounts (Sharma, 2020). The adoption of smartphone privacy tools is influenced by user awareness and education on security measures (Alashi & Aldahawi 2020). Enhancing the clarity of privacy policies within apps can build user trust (Zhang et al., 2020). With smartphones playing a role in daily routines, effective privacy management tools are increasingly vital (Sharma, 2020). By incorporating tools that provide transparency and control over data exposure, developers empower users to make choices

regarding their online privacy (Carelli et al., 2019). Using privacy tools on smartphones is essential, for minimizing privacy risks and safeguarding information in today's digital landscape.

Growing concerns regarding data security and privacy have sparked a rise in the popularity of privacy focused smartphone applications in recent years, and 95.2% of the survey respondents reported being concerned about the privacy and protection of their personal data on smartphones (Mylonas et al., 2013). Research has highlighted the role of security awareness in combating malicious apps and enhancing user safety on smartphone platforms (Mylonas et al., 2013). Addressing privacy issues is key to fostering trust and reducing perceived risks associated with location-based services (Zhou, 2011). Studies emphasize the importance of tools for safeguarding user data and establishing user confidence in smartphone security and privacy (Chin et al., 2012). Developing models and tools prioritizing privacy is essential to mitigate privacy risks and protect user information effectively (Benthall et al., 2022). Efforts to bolster user security and privacy without compromising usability in smartphone apps aim to incorporate technologies that enhance privacy protection (Hatamian, 2020).

Understanding how users interact with privacy policies and tools is vital for enhancing user awareness and engagement with privacy settings, on smartphones (Ullah et al., 2022). Many Android apps require permissions to access sensitive data and resources on the user's device, and most users do not pay attention to these permission requests and allow access, which can lead to privacy risks and data leakage. The study found that out of over 25,000 app downloads, only about 22% of users visited the privacy policy page of the apps. This shows that most users need to read and understand how their data may be collected and used. Despite the sensitive permissions requested by apps, users' low engagement with privacy policies highlights a major risk to user data privacy on smartphones. Understanding this behavior is the first step towards developing better approaches to engage users and safeguard their privacy (Ullah et al., 2022).

In today's era, there is a growing recognition of the significance of safeguarding privacy and addressing user concerns. This shift is evident in the emergence of privacy focused smartphone applications (Bakar et al., 2021). Smartphones' common privacy tools and settings offer features that empower users to manage their data and protect their privacy effectively. For instance, one key tool is app permission control, allowing users to choose which permissions apps can access, such as contacts, camera, or location (Ramokapane et al., 2019). Privacy settings often include options for managing ad tracking limiting data sharing with parties and controlling personalized

advertising (Barth S., 2021). Additionally, default features are provided by manufacturers of smartphones. Like data sharing controls and location services. Play a role in enhancing user privacy (Ramokapane et al., 2019). Personalized privacy assistants are another asset that offers tailored recommendations for privacy settings based on individual behavior and preferences (Carter, 2022). These assistants leverage user modeling and machine learning techniques to suggest personalized strategies for enhancing smartphone privacy controls (Carter, 2022).

Users can control their privacy settings and preferences with the help of tools like privacy panels and customization features (Zhou et al., 2017). Crowdsourced recommendation engines are designed to suggest privacy settings based on user preferences and behaviors to enhance user awareness and control over their privacy (Harborth et al., 2019). Smartphone applications integrate location-based privacy settings and privacy preserving cache models to safeguard user data when sharing location information (Patel & Palomar, 2016). These tools allow users to customize permission settings to protect their privacy using location-based services (Patel & Palomar, 2016). By dispelling misconceptions and providing resources, smartphone users can make informed decisions about their privacy settings and data sharing practices. The focus on developing smartphone privacy tools reflects a conscious effort to empower users to manage their digital privacy effectively. Smartphone users can make informed choices about their privacy settings and how they share their data by dispelling misunderstandings and providing helpful resources to guide decisions on privacy matters (Kulyk et al., 2019).

2.3 Factors influencing Adoption and Usage of privacy Tools

The factors influencing the adoption and use of privacy tools in smartphone usage vary and involve different demographic factors. According to a study by Meier et al. (2021), privacy concerns play a role in decision-making when using privacy tools. Tsetsi & Rains (2017) indicate that individuals from minority age groups, those with lower incomes and less educated users, are more likely to rely heavily on smartphones, which could affect how they adopt privacy tools. Recent research has highlighted how factors, cybersecurity knowledge, and the use of privacy tools impact individuals' behaviors. Age stands out as a factor influencing how people approach cybersecurity practices and make choices about using privacy tools, according to Addae et al. (2019). Studies suggest that older individuals may have limited cybersecurity knowledge, potentially affecting their interactions with privacy tools meant to protect information (Lyon,

2023). Moreover, demographic characteristics like age can shape how people safeguard their privacy - a point emphasized in cybersecurity awareness efforts focused on age-related aspects by Weinberger et al. (2017). The relation between age and cybersecurity knowledge has also been explored in relation to utilizing privacy tools.

Research indicates that older people may need to be more well-informed about cybersecurity practices as individuals, potentially affecting their willingness to use privacy tools (Lyon, 2023). It is essential to understand how factors like age, knowledge of cybersecurity, and the use of privacy tools to design targeted educational programs and interventions that raise awareness of digital privacy risks and encourage the effective utilization of privacy-enhancing technologies (Pratama et al., 2022). Considering age related differences in cybersecurity knowledge and attitudes toward privacy, can help organizations and policymakers develop strategies to improve privacy practices across different age groups. Privacy risks are becoming increasingly concerning, particularly for smartphone users. Studies have pointed out a need for more awareness among smartphone users regarding security and privacy risks associated with applications and services (Alsaleh et al. 2017). The abundance of smartphone apps and a lack of comprehension about risks present significant obstacles to user privacy (Alsaleh et al., 2017). Moreover, using smartphones in healthcare emphasizes the need to address digital privacy risks effectively to safeguard against unauthorized access to sensitive information (Nettrour et al., 2019).

Raising awareness about the dangers is vital in empowering individuals to make informed choices regarding their online interactions and safeguarding their sensitive information from potential breaches (Alsaleh et al., 2017). Studies indicate a necessity for educating users, including the elderly, on digital privacy threats to ensure the safe and secure usage of mobile devices (Shuijing & Jiang 2017). Elderly individuals might face risks related to privacy due to potentially lower levels of digital literacy, making them more prone to privacy infringements (Shuijing & Jiang 2017). Recognizing the digital privacy challenges encountered by various user demographics like seniors is crucial for creating targeted education campaigns and initiatives to reduce these risks (Shuijing & Jiang 2017). By promoting awareness about privacy threats and offering guidance on safe smartphone practices, individuals can enhance the protection of their personal data and decrease the chances of experiencing privacy breaches (Shuijing & Jiang 2017).

Various aspects, including demographics, knowledge, education, and privacy concerns, impact how people use smartphone privacy tools. Studies indicate that individuals' understanding of their privacy influences how they behave in different scenarios (Padyab et al., 2019). The decision to use privacy tools is influenced by perceived advantages and personal willingness to try things, suggesting that personal traits can sway users' decisions (Duan & Deng 2022). Users' sense of control over their information is tied to their level of knowledge about privacy issues emphasizing the importance of education in empowering individuals to protect their privacy (Prince, 2024).

It has also been observed that the alignment of mobile app services with privacy concerns affects how willing people are to use those apps, underscoring the need to consider privacy matters when designing services (Hsieh & Li 2021). The research by Hsieh and Li (2021) introduces the concept of service-privacy fit (SPF), which means the perceived degree of match between the service offered by a mobile app and the privacy permissions it requests from users. Their key findings suggest that SPF significantly influences users' willingness to adopt and use a mobile app. When users perceive a good fit between the app's service and privacy requirements, they are likelier to download and use the app. Also, perceived mismatch or poor SPF can deter users from adopting the app. It has been recognized that incorporating gamification can contribute to safeguarding user privacy by increasing awareness about privacy challenges and enhancing user involvement (Mavroeidi et al., 2020).

Several factors, like influence from peers' permissions for devices and apps, social conventions, and reliance on technology providers, impact how people adopt and use smartphone privacy tools. Users often base their decisions on whether to use privacy tools on how they trust the technology providers. They are more inclined to use tools they believe will effectively safeguard their data as noted by Singh et al., (2024). User's concerns about privacy may be influenced by the permissions granted to devices and applications, prompting them to exercise caution when allowing access to sensitive information (Ullah et al., 2022). The influence of peer pressure and societal norms significantly shapes individuals' behavior concerning privacy tools. Studies have highlighted how social norms impact users' attitudes and actions regarding privacy practices, emphasizing the role of expectations in privacy-related decision-making (Wolff, 2023). Since individuals often seek peer advice, peer influence can impact perceptions of privacy and willingness to embrace privacy tools (Dogruel et al., 2022). Therefore, several key factors such as

peer pressure, adherence to norms, trust in technology providers, and careful consideration of permissions play a pivotal role in the adoption and utilization of privacy tools in smartphone usage. Understanding these factors is essential for developing strategies that promote privacy protection and empower users with control over their data.

2.4 Differences in Privacy tool usage Across Smartphone platforms

Kollnig et al. (2021) conducted a study comparing Android applications, uncovering potential breaches of privacy laws such as unauthorized tracking by third parties and insufficient data protection measures. This research emphasizes the importance of examining privacy practices on both platforms to ensure adherence to regulations and safeguard user data. The study by Ubhi et al. (2017) delved into the characteristics and behaviors of users on iOS and Android, specifically focusing on contexts like smoking cessation apps. Their findings offer insights into user preferences and behaviors across different platforms, which can impact adopting privacy tools. Additionally, Kollnig et al. (2021) also identified privacy law violations on both platforms, including issues like tracking and inadequate data protection measures. This comparative analysis sheds light on the existing challenges in privacy practices for iOS and Android apps, highlighting the necessity for enhanced privacy features and transparency to protect user data effectively. The paper highlights several key challenges in the privacy practices of iOS and Android apps such as lack of transparency around apps' data practices, widespread potential infringements of privacy laws, conflicts of interest for platform owners where Apple and Google have a financial interest in allowing app publishers to collect user data to drive sales, from which the platforms take a share of the revenue. Differences between platforms that impact privacy were another challenge. The study found Android apps tended to share potentially invasive persistent identifiers like the Advertising ID more often than iOS apps.

iOS and Android platforms exhibit approaches to privacy features. iOS stands out for its privacy policies prioritizing user privacy as a core aspect (Paul, 2022). Apple's system prioritizes safeguarding user information, with the company reviewing each app to ensure data privacy (Feng et al., 2019). On the one hand, Android emphasizes users taking responsibility for checking permissions, putting the onus on them to protect their privacy (Feng et al., 2019). This approach also reflects how developers perceive privacy on each platform; iOS developers often focus on obtaining user consent and providing information, aligning with Apple’s strong stance on privacy.

In contrast, Android developers see privacy as an added feature to set their apps apart in the competitive market (Tahaei et al., 2020). Moreover, a comparison of privacy statements between iOS and Android apps revealed that statements on iOS tend to be slightly longer than those on Android (Shaw et al., 2022). This discrepancy in statement length may indicate a thorough and detailed approach to disclosing privacy practices on the iOS platform. Additionally, while Android's flexibility and customization options are appealing, they make it vulnerable to malware that exploits security weaknesses (Alkahtani & Aldhyani 2022). This highlights a challenge for Android in maintaining an open ecosystem while ensuring robust security measures to protect users from potential risks.

Studies have indicated that users of iOS devices are often more conscious about their privacy than those using Android, showing an awareness and concern for safeguarding their data privacy (Kollnig et al., 2022). This heightened attention among iOS users stems from Apple's focus on privacy features and transparency, such as the App Tracking Transparency framework, which empowers users to manage their data and tracking preferences effectively (Kollnig et al., 2022). On the one hand, research suggests that Android users may have a more relaxed approach toward privacy, possibly due to the platform historically offering users greater freedom in app permissions and data-sharing practices (Ramokapane et al., 2019). The contrast in privacy attitudes between iOS and Android users highlights the significance of comprehending user behaviors and preferences to customize privacy features, for each platform.

In a comparative study by (Kollnig et al., 2021), the privacy features of iOS and Android apps were assessed, revealing that about 59% of Android apps shared the AdId with third parties over the internet, compared to 25% on iOS. This finding underscores a potential privacy vulnerability in Android apps concerning data sharing practices. By comparing the privacy footprints of iOS and Android apps, this study sheds light on the differences in privacy protection between the two platforms, indicating areas where Android may lag behind iOS in safeguarding user privacy. Reinfelder et al. (2014) explore the differences between Android and iPhone users in terms of security and privacy awareness. Understanding user perceptions and behaviors towards security and privacy is crucial in tailoring privacy features to meet user expectations on both platforms. By examining user awareness levels, this study contributes valuable insights into how iOS and Android can enhance their privacy features to align with user preferences and improve overall privacy protection for users of both operating systems.

Research by Chin et al. (2012) emphasizes the importance of user confidence in smartphone security and privacy, highlighting the need for secure smartphones that enable users to benefit from mobile platforms safely (Chin et al., 2012). Understanding user confidence and perceptions is essential for designing secure smartphones that align with user expectations and enhance privacy protection. Studies like Sudirman et al. (2023) provide insights into the information security behaviors of smartphone users, indicating that user awareness and behaviors differ based on the operating system they use. A few of their study findings are that Android users behave more safely than iOS users in avoiding harmful behavior, and iOS users behave more securely than Android users in adopting settings and add-on utilities, preventive behavior, and disaster/data recovery. Post-hoc analysis showed that when it comes to automatically backing up data in the cloud, iOS users have better behavior than Android users. By identifying these differences, developers, and policymakers can implement targeted measures to enhance security and privacy practices among Android and iPhone users. Research on privacy awareness, such as (Alani, 2017), underscores the importance of ongoing efforts to educate users about privacy risks and best practices to mitigate potential security threats.

2.5 Role of Digital Forensics and Law Enforcement

Exploring the factors influencing the adoption and usage of privacy-enhancing tools among smartphone users is crucial for law enforcement. Research in this area can provide insights into user behaviors, preferences, and concerns regarding privacy tools, which can inform the design and implementation of more robust privacy solutions (Crossler (2011); Bracamonte et al., 2022; Maceli, 2018). The usability of default smartphone features and user privacy considerations can impact law enforcement interactions, as users' awareness and management of privacy settings influence data availability for investigative purposes (Ramokapane et al., 2019). Adopting privacy-enhancing technologies, such as Global Privacy Control, reflects a growing trend toward empowering users with greater control over their data, potentially limiting law enforcement access (Zimmeck et al., 2023).

By exploring factors such as performance expectancy, social influence, privacy concerns, and privacy self-efficacy, studies can offer valuable information on user intentions to use privacy-sensitive tools, aiding in developing tools that align with user needs and expectations (Bracamonte et al., 2022). Additionally, understanding the knowledge gaps in user’s comprehension of internet

infrastructure and privacy tools can help bridge the information gap between users and service providers, enabling users to make more informed decisions about their privacy (Maceli, 2018). Moreover, research on digital forensics frameworks and encryption techniques can contribute to enhancing the privacy-preserving capabilities of investigative processes, ensuring that digital forensics professionals can effectively collect and analyze evidence while respecting privacy rights (Halboob & Al-Muhtadi, 2023; Pourvahab & Ekbatanifard, 2019; Alendal et al., 2021).

Understanding these factors can provide valuable insights into user behaviors, preferences, and concerns regarding privacy tools, which can inform the development of more effective privacy solutions (Stamm & Liu 2011; Karie & Venter, 2015). For digital forensics professionals, this exploration can offer insights into the privacy tools commonly used by smartphone users, enabling them to understand better the digital footprint left by individuals and the potential challenges in collecting evidence from privacy-enhanced devices (Ramadhan et al., 2022; Yudhana et al., 2019). Understanding how individuals secure their data on mobile devices equips investigators with the necessary knowledge to address challenges in evidence collection from privacy-enhanced devices. This knowledge is fundamental for upholding the integrity and efficacy of digital forensic investigations in an increasingly privacy-conscious digital environment. The privacy implications of smartphone data collection, particularly in health research applications, raise worries about unregulated privacy breaches and potential harm to individuals (Tovino, 2020).

By comprehending the factors that influence the adoption of these tools, digital forensics experts can adapt their investigative methodologies to account for the privacy measures implemented by smartphone users, ensuring a more thorough and legally sound investigation process (Montasari, 2017; Alendal et al., 2021). Similarly, for law enforcement individuals, understanding the factors that drive the adoption of privacy-enhancing tools can shed light on the evolving landscape of digital privacy and the challenges faced in digital investigations (Obidzinski & Oytana, 2018; Smernytskyi et al., 2021). This knowledge can aid law enforcement agencies in developing strategies to navigate privacy concerns while conducting investigations, ensuring that legal procedures are followed and evidence is obtained ethically and effectively (Panova et al., 2020; Alghamdi, 2021).

To effectively investigate cyber incidents such as privacy breaches and data security concerns, digital forensics, and law enforcement play a role, according to Stoyanova et al. (2020) and Garfinkel (2010). By utilizing models and frameworks in the field of digital forensics science

law enforcement agencies can efficiently collect and analyze digital evidence related to the usage of privacy enhancing applications on smartphones (Stoyanova et al., 2020; Garfinkel, 2010). Integrating privacy enhancing tools into smartphone use poses privacy challenges that digital forensics must address, as highlighted by Arshad et al. (2022) and Halboob & Al Muhtadi (2023). Ensuring the protection of privacy rights during investigations requires a balance between technical aspects and legal considerations in automating digital forensics processes (Arshad et al., 2022; Halboob & Al Muhtadi 2023). In cybercrime cases associated with smartphone privacy enhancing apps law enforcement agencies need to establish protocols and guidelines for handling situations (Anggraeny et al., 2022; Sibe & Muller 2022). By adhering to practices and standards, in digital forensics law enforcement can effectively address the complexities involved in investigating privacy related incidents (Anggraeny et al., 2022; Sibe & Muller 2022).

Integrating frameworks into digital inquiries is essential to ensure that investigations are conducted ethically and in compliance with the law (Ieong, 2006; Halboob & Al Muhtadi 2023). By adopting this approach, law enforcement agencies can effectively. Assessing digital evidence while upholding individual privacy rights (Ieong, 2006; Halboob & Al Muhtadi 2023). Considering aspects enhances the acceptance and trustworthiness of evidence presented in court, thereby bolstering public faith in law enforcement's commitment to safeguarding digital privacy (Ieong, 2006; Halboob & Al Muhtadi 2023). Collaboration between law enforcement bodies and the technology industry is crucial to enhancing smartphone privacy features and advancing forensic capabilities (Ieong, 2006; Halboob & Al Muhtadi 2023). Law enforcement gains valuable insights into the latest privacy-protecting methodologies by establishing partnerships with tech firms. This collaboration ensures that investigations prioritize privacy safeguards utilizing state-of-the-art approaches (Ieong, 2006; Halboob & Al Muhtadi 2023).

This collaboration allows the tech industry to receive insights on implementing privacy tools effectively in real world investigative situations while providing law enforcement access to advanced technological resources. Balancing security and privacy is challenging for law enforcement agencies engaged in digital investigations. Striking the balance between security measures and privacy protection is essential to prevent privacy breaches, combat cybercrime efficiently, and ensure public safety. By adopting an approach that addresses security and privacy concerns, law enforcement can maneuver through the intricacies of digital investigations with

honesty, transparency, and a firm dedication to upholding privacy rights in compliance with legal and ethical norms.

2.6 Summary

This chapter explores the existing literature and provides an overview of digital privacy challenges, evolution, and development of privacy-enhancing tools such as encryption, VPNs, and ad blockers. The chapter then delves into the factors influencing the adoption and usage of privacy-enhancing tools and discusses various demographic factors such as age, education level, and cybersecurity knowledge. Further, the differences across smartphone platforms were highlighted, where iOS and Android exhibit contrasting approaches to privacy, with iOS prioritizing user privacy more strongly. Studies indicate differences in data sharing practices, user awareness, and attitudes toward privacy across the two platforms. We reviewed the role of digital forensics and law enforcement, as understanding user adoption of privacy tools is crucial for digital forensics and law enforcement investigations. Collaboration between law enforcement and the tech industry can enhance privacy features and forensic capabilities. The review highlights the importance of addressing digital privacy, understanding user behaviors, and developing robust privacy-enhancing solutions while navigating legal and ethical considerations in the smartphone era.

3. METHODOLOGY

This chapter provides an overview of the research design and methodology used. The research followed a quantitative survey model consisting of questions related to demographics, privacy tools usage, privacy concerns, privacy risks, smartphone operating systems, and familiarity with cybersecurity. The survey received IRB approval (IRB #2024-326). Participants were recruited to participate in the survey via Mturk. The participant criteria were set to the population above 18 years of age and located in the United States. The questions were of yes or no type, five-point Likert scale type where five options were arranged from least to most concerned, multiple-choice question for operating system related questions and choose multiple options for tools question, and text analysis questions. The data was analyzed to understand the primary reason for the participants to use privacy-preserving tools. More details of survey design, sampling, measures, and analytical strategy are discussed in this chapter below.

3.1 Research Question

The research questions for this study are:

1. How prevalent is the use of privacy-enhancing tools and settings among smartphone users?
2. What factors influence users' adoption and usage of privacy-enhancing tools?

3.2 Hypotheses

The hypotheses for this study are:

1. There is a significant difference in the use of privacy tools among smartphone users based on demographic factors such as age, education level, and occupation.
2. Smartphone users with a higher awareness of digital privacy risks are likelier to use privacy-enhancing tools and settings on their devices.
3. The prevalence and type of privacy tools used differ significantly between iOS and Android smartphone users.

3.3 Survey Design

This research explored behaviors around privacy-preserving technologies. The research study was conducted using quantitative and qualitative survey methods and hosted on Qualtrics. Participants were recruited from Amazon MTurk. The survey consisted of a questionnaire attached in Appendix D, where participants were asked to provide some of their demographic information, followed by responses to the questionnaire about privacy-preserving technologies. Respondents were solicited automatically by MTurk, based on inclusion criteria. This solicitation in Appendix C includes a survey link that takes respondents to start the survey if they are interested in participating. This link was directed to Purdue University's Qualtrics website, where the entire study procedure occurred. The opening page of the Qualtrics survey included the informed consent attached in Appendix C. If respondents chose to proceed with participation, they were directed to the survey after clicking the link. There was no direct or indirect contact between researchers and potential participants. No identifying information was collected during the entire research. Only individuals 18 and older and currently residing in the United States were eligible to complete the study. Following this, participants were given a questionnaire measuring privacy preserving technology use. In addition, the survey employed reCAPTCHA and embedded data within Qualtrics to prevent automated responses from bots.

The survey included sixteen questions, where the first two questions were related to demographics on age and gender, followed by cybersecurity knowledge and familiarity with security features questions taken from Breitinger et al., (2020). Privacy concern questions were taken from Kalkos et al., (2021) and provided Likert scale where one being not concerned at all and five being strongly concerned. Questions about options for privacy tools were taken from Story et al., (2021) and Dixon et al., (2023). Smartphone OS and device questions were taken from Abrokwa et al., (2021). Data privacy and privacy risk yes or no questions were added to know about privacy risks as knowing about the prevalence of the usage of privacy-preserving tools based on demographic factors helps this study. The study helps understand smartphone OS and attitudes towards what privacy tools were used. The research team aimed to study cybersecurity awareness and privacy risks with privacy tools, and once the responses were collected, statistical analysis was conducted.

The survey was designed in such a way that it collected data regarding age, gender, smartphone OS, familiarity with cybersecurity, affected by a data privacy breach or not, concern

about online privacy, concern about personal information being misused, concern about personal information could be accessed by unknown parties, heard about digital privacy risks, what is the biggest digital privacy risk, select the tools that participants are using on their phone and what is their primary reason for using privacy-preserving tools, how familiar are the participants with the security features and default settings on the smartphone, knowing if the participants primary smartphone devices are rooted or jailbroken.

3.4 Sample

IRB approval was received from the Purdue University Institution Review Board for the survey under the number IRB-2024-326. The study aimed to recruit participants aged 18 and above from those residing in the United States. Amazon MTurk was utilized to recruit participants. The Purdue University Department of Computer and Information Technology funded participants with 0.75$ each for completing the survey. When recruiting respondents from Amazon Mechanical Turk (MTurk) for a survey aimed at the US population over the age of 18. MTurk participants are much more diverse than average American college samples and marginally more diverse than conventional internet samples, according to a study by Buhrmester et al. 2011. Despite variations in compensation rates and task lengths, MTurk remains a rapid and cost-effective method for participant recruitment (Buhrmester et al., 2011).

Researchers can leverage MTurk's reputation system and secure payment methods to ensure data quality and participant engagement (Chandler et al., 2019). While MTurk offers a convenient platform for data collection, researchers should be aware of its limitations. MTurk gives users access to a varied sample that roughly resembles the whole population, however some demographic traits might only be partially captured (Contractor et al., 2023). For instance, Buhrmester et al. (2011)'s study discovered that MTurk employees are typically younger, better educated, and more tech-savvy than the general population. To address this, researchers employ statistical weighting techniques to adjust the sample data for better representativeness (Buhrmester et al., 2011). Moreover, MTurk has been utilized successfully in various research fields, including addiction research and mental health studies (Mellis, & Bickel, 2020; Kim, & Hodgins, 2017). By carefully designing Human Intelligence Tasks (HITs), verifying participant eligibility, and incorporating attention check questions, researchers can enhance the validity and reliability of survey data collected through MTurk (Levay et al., 2016).

3.5 Analytical Strategy

3.5.1 Data Screening

IBM SPSS version 29 was used to analyze the data and eliminate unusable responses from 1,200. The survey platform, Qualtrics, automatically screened out participants based on predefined criteria such as being under 18, residing outside the U.S., failing bot detection, and captcha verification. The data cleaning process in SPSS involved several steps to refine the initial pool of 1,200 responses. The data was imported into SPSS to eliminate unusable data. Initially, 90 responses that chose "do not agree" for the survey consent were deleted, resulting in 1,110 responses. 147 responses were deleted based on the ReCAPTCHA score, resulting in 963 responses. 620 cases were found with missing data on quantitative questions. Removed all these responses with any sort of missing data on quantitative questions, resulting in 343 responses. One response was deleted because of a duplicate response from the same respondent, resulting in 342 responses. The final dataset was refined down to 342 responses.

3.5.2 Statistical Methods

The research, conducted using both quantitative and qualitative methods, considered 342 samples as usable responses. IBM SPSS version 29 was used for statistical analysis to determine the significance of the hypothesis supporting the first research questions. Microsoft Excel was used to perform content analysis for the context question in the survey to support the second research question. The research questions for this study as stated in Chapter 1 are “How prevalent is the use of privacy-enhancing tools and settings among smartphone users?” and “What factors influence their adoption and usage?”. The declared three hypotheses would help research the declared research question.

To investigate the prevalence of privacy-enhancing tools and settings among smartphone users, the study analyzed the relationship between demographic factors such as age and familiarity with cybersecurity and the total number of tools used. Cramer’s V Correlation was employed to assess the association between age and the total number of tools used, categorized as none, low, or high. Spearman’s Correlation was utilized to examine the correlation between familiarity with cybersecurity and the total number of tools used.

To investigate whether smartphone users with a higher awareness of digital privacy risks are more likely to use privacy-enhancing tools and settings, the study utilized statistical tests on survey questions related to privacy risks, privacy tools, and security features. Specifically, the Phi test was employed to evaluate the significance between privacy risk and privacy tools. In contrast, Cramer's V correlation test was used to analyze the relationship between privacy risk and security features. The study benefits from previous research exploring user behaviors and attitudes toward smartphone privacy and security. Understanding users' security awareness and behaviors in smartphone platforms can provide insights into the level of complacency and trust among users regarding security controls and app repositories Mylonas et al. (2013). Additionally, investigating users' behavior toward application privacy policies can show how users interact with privacy-related information and permissions (Ullah et al., 2022). Kruskal-Wallis test was performed for the survey questions "Smartphone OS" (What operating system do you have on your smartphone?) and "Privacy Tools 2" (Please select any of the following tools you use on your phone).

3.5.3 Content Analysis for text responses

Qualitative inductive content analysis was used to analyze the text responses (Snir et al., 2022), by highlighting keywords and phrases related to privacy risks and reasons for using privacy tools. The content analysis uses individual codes to describe the unit for analysis instead of using entire sentences given by the user (Zhang, Y. & Barbara, M. (2005)), where a code refers to a meaningful and recurrent pattern or concept that is identified within the data and serves as a unit of analysis, rather than analyzing the data as complete sentences or responses. The author familiarized themself with all the data from text responses by reading the text responses, identifying relevant data, and conducting inductive reasoning to highlight keywords and phrases related to privacy risk concerns and reasons for the usage of privacy-enhancing tools. The data was categorized into meaningful codes to facilitate analysis. The process involved organizing the data systematically, and coding responses into categories of privacy risks (Graneheim & Lundman, 2004). After the initial coding, the author grouped similar codes into broader categories. All the data were categorized into meaningful categories and sorted into smaller numbers of higher-order headings (Elo & Kyngäs, 2008).

To answer the research question regarding the factors influencing the users' adoption and usage of privacy-preserving tools, the survey asked text questions asking the users about what they consider the biggest privacy risk and what their primary reason for adopting and using privacy-preserving tools to understand their motivations and reasons. Users' responses to these two questions were included in the analysis, "What would you consider to be the biggest digital privacy risks to you? Else type N/A.", and "What is your primary reason for using privacy-preserving tools?". The findings from this analysis were reported in sections 4.4.1 and 4.4.2, detailing the insights gained regarding digital privacy risk concerns and the primary reasons for using privacy-preserving tools. This structured approach to content analysis aids in identifying key factors influencing users' adoption and usage of privacy tools, providing valuable insights for research and decision-making in data privacy and security.

3.6 Summary

The research objectives, survey design, sampling procedures, and analysis to evaluate significant variables, including age, cybersecurity familiarity, privacy tool usage, security features, Smartphone OS, and main motivations for incorporating privacy-preservation tool usage are all outlined in this chapter. 342 valid responses were collected through MTurk, and Qualtrics was used to manage the online survey. The analytical strategy used in this study is also covered in detail in this chapter. IBM SPSS Version 29 was used to process the collected data.

4. RESULTS

This chapter presents the findings of the study through descriptive statistics. It describes the sample characteristics regarding demographics, outlines the measures used, and discusses the statistical analyses conducted. Furthermore, it delves into the final analyses employed to test the hypotheses.

4.1 Data Analysis

Testing outliers and assumptions are important for hypothesis testing as it helps ensure the validity and reliability of the statistical analyses and conclusions drawn from the data. The variables considered for testing are age, familiarity, total tools usage, privacy risks, privacy tools, security features, and smartphone operating system. 23 different outliers were present for all the testing variables, approximately 6.7 %. The outliers were not removed from the study. The variables used for testing the hypotheses did not meet the assumptions of normality, homogeneity of variance, and linearity tests, resulting in the use of non-parametric tests.

Levene's test indicated unequal variances for "Total tools used" based on age ($F = 336$; $p = 3.395$). For familiarity with cybersecurity, variances were not significantly different for the mean ($F = 2.547$, $p = .039$), for "Security features usage with aware of privacy risks," variances were different for the mean ($F = 4.252$, $p = .040$). Refer to Table 4.5 for the homogeneity of variance assumption test.

Table 4.1 Assumption Testing for Variables – Homogeneity of Variances

Tests of Homogeneity of Variances		Levene Statistic	df1	df2	Sig.
Total tools used vs Age	Based on Mean	3.395	5	336	0.005
	Based on Median	3.214	5	336	0.008
	Based on Median with adjusted df	3.214	5	323.420	0.008
	Based on trimmed mean	3.242	5	336	0.007
Total tools used vs Familiarity with cybersecurity	Based on Mean	2.547	4	337	0.039
	Based on Median	2.423	4	337	0.048
	Based on Median with adjusted df	2.423	4	325.346	0.048
	Based on trimmed mean	2.245	4	337	0.064
Usage of Privacy tools vs aware of privacy risk	Based on Mean	50.022	1	340	0.000
	Based on Median	11.630	1	340	0.001
	Based on Median with adjusted df	11.630	1	156.293	0.001
	Based on trimmed mean	22.456	1	340	0.000
Security features usage with aware of privacy risks	Based on Mean	4.252	1	340	0.040
	Based on Median	2.090	1	340	0.149
	Based on Median with adjusted df	2.090	1	339.693	0.149
	Based on trimmed mean	5.440	1	340	0.020

4.2 Descriptives

The survey was conducted through Mturk to assess various factors related to digital privacy and security practices among smartphone users, and a total of 342 valid responses were collected. Variables of interest used for hypotheses testing described in this section are age, smartphone OS, familiarity with cybersecurity, most used privacy tools, device security settings, and overall privacy tool usage. Most respondents (56.1%) were in the 24-30 age group, followed by 24.9% aged 31-40, 7.9% aged 41-50, 6.4% aged 18-23, 2.9% aged 51-60, and 1.8% over 60. 74.3% of respondents identified as male and 25.7% as female (Table 4.2).

Table 4.2 Demographics – Age and Gender

Age	N	Percent %
18 - 23	22	6.4
24 - 30	192	56.1
31 - 40	85	24.9
41 - 50	27	7.9
51 - 60	10	2.9
Over 60	6	1.8
Total, N	342	100
Gender	**N**	**%**
Male	254	74.3
Female	88	25.7
Total, N	342	100

Regarding smartphone usage, Android was the most common smartphone operating system, used by 74.3% of respondents. 11.7% used iOS, 12.6% used Android and iOS, 1.2% did not have a smartphone, and 0.3% used another operating system (refer to Table 4.3). Cybersecurity Knowledge and Experiences: 40.9% of respondents reported reading about or self-taught cybersecurity topics, while 31.3% followed related news. 12.3% had taken a course or earned a certification, 9.6% had a degree in a related field, and 5.8% did not know the topics. A large majority (78.7%) reported being affected by a data privacy breach (refer to Table 4.4).

Table 4.3 Smartphone OS

Smartphone OS	N	%
iOS	40	11.7
Android	254	74.3
I do not have a smart phone	4	1.2
I use both iOS and Android	43	12.6
Other	1	0.3
Total, N	342	100

Table 4.4 Familiarity with Cybersecurity

Familiarity Cybersecurity	N	%
1 - I have no knowledge of related topics	20	5.8
2 - I follow the news of related topics	107	31.3
3 - I have read/taught myself about related topics	140	40.9
4 - I have taken one or more courses in a related topic or have a certification	42	12.3
5 - I have a degree in this or a related field	33	9.6
Total, N	342	100

Almost all respondents (97.4%) reported using at least one privacy-preserving tool on their smartphone. The most used tools were password managers (67.8%), antivirus software (47.7%), privacy-focused browsers (46.8%), VPNs (39.8%), ad blockers (37.1%), encryption apps (35.4%), and locked folders (33%). For device security settings, most respondents (76.9%) reported having thoroughly checked their phone's security settings, 20.2% made changes as issues came to their attention, and 2.9% used default options. 76% said their device was not rooted or jailbroken, 20.2% said it was, and 3.8% were unfamiliar with the terminology. Using IBM SPSS, total tools used by each participant were added and categorized as none for 0, low usage for 1,2, and high usage for 3 and above total tools used. 65.2% of respondents had high overall privacy tool usage, while 34.5% had low usage (refer to Table 4.5).

Table 4.5 Privacy Practices and Tools Usage

Most Used Privacy Tools	Number	Percent
Password Managers	232	67.8
Antivirus Software	163	47.7
Privacy-focused Browsers	160	46.8
VPNs	136	39.8
Ad Blockers	127	37.1
Encryption Apps	121	35.4
Locked Folders	113	33
Device Security Settings		
Thoroughly checked settings	263	76.9
Make changes as needed	69	20.2
Uses default options	10	2.9
Device Rooting/Jailbroken		
Not rooted/jailbroken	260	76
Rooted/Jailbroken	69	20.2
Unfamiliar with terminology	13	3.8
Overall Privacy Tool Usage		
High Usage (3 + tools)	223	65.2
Low Usage (0 - 2 tools)	118	34.5
None	1	0.3
Total, N	342	100

4.3 Hypotheses Testing

This section discusses data analysis and testing of hypotheses declared for the study.

4.3.1 Hypothesis 1:

The study's first hypothesis states, “There is a significant difference in the use of privacy tools among smartphone users based on demographic factors such as age and familiarity on

Cybersecurity". Age, familiarity, and total tool usage were considered to test this hypothesis. To test the significance between age and usage of privacy tools, Cramer's V test is followed to know the significance. The Cramer's V value is 0.232, indicating a strong association between age and privacy tool usage as per Akoglu (2018). The approximate significance ($p < 0.001$) is statistically significant. This supports rejecting the null hypothesis of no association between the two variables. The Cramer's V correlation analysis suggests a strong association between age and privacy tool usage among the study participants. Where the age increases, privacy tools usage decreases. The crosstabulation provides a more detailed picture of the distribution of privacy tool usage across age groups, with younger age groups showing a higher proportion of "High Usage" than the older age groups. These results support the hypothesis that there is a relationship between age and privacy tool usage. (refer to Table 4.6)

Table 4.6 Cramer's V test for Age vs Total tools Usage

Cramer's V		Value	Significance
Nominal by Nominal	Cramer's V	0.232	<.001
N of Valid Cases		342	

Familiarity with cybersecurity and usage of privacy tools follows Spearman's Rho correlation test to know the significance. Spearman's Rho correlation was used, and the results are shown in the table below. The Spearman's Rho correlation coefficient between "How familiar are you with cybersecurity (on a scale of 1-5)?" and "Total tools used" is 0.256, which indicates a weak positive monotonic correlation between the two variables as per Akoglu (2018). As familiarity with cybersecurity increases, there is a slight tendency for the total number of privacy tools to increase. The correlation coefficient is statistically significant at the 0.01 level (2-tailed). The significance level (p-value) for the correlation coefficient is reported as ($p < .001$), less than the conventional significance level of 0.05. This further supports the conclusion that the correlation between familiarity with cybersecurity and the total tools used is statistically significant. The analysis found a weak positive monotonic correlation between familiarity with cybersecurity and privacy tool usage (" = 0.256, $p < .001$, $N = 342$). Though the correlation is statistically significant,

the strength of the association, being 0.256, suggests that other factors may also play a role in determining privacy tool usage (refer to Table 4.7).

Table 4.7 Spearman's Rho correlation for Familiarity vs Total tools used

Correlation			Familiarity with cybersecurity	Total tools used
Spearman's rho (")	Familiarity with cybersecurity	Correlation Coefficient	1.000	.256**
		Sig. (2-tailed)	.	<.001
		N	342	342
	Total tools used	Correlation Coefficient	.256**	1.000
		Sig. (2-tailed)	<.001	.
		N	342	342

**. Correlation is significant at the 0.01 level (2-tailed).

The results show a significant difference in the use of privacy tools among smartphone users based on demographic factors such as age and familiarity with cybersecurity, supporting the hypothesis.

4.3.2 Hypothesis 2:

The study's second hypothesis states, "Smartphone users with a higher awareness of digital privacy risks are likelier to use privacy-enhancing tools and settings on their devices." To test this hypothesis, the questions Privacy Risk 1 (Have you heard of the term "digital privacy risks"), Privacy Tools 1 (Do you currently use any privacy-preserving tools on your smartphone?) (refer to Appendix D) were considered, where both being dichotomous variables and Phi test is suitable for both variables being dichotomous, the results are shown in Table 4.8.

The Phi coefficient (φ) is 0.182, indicating a strong association between privacy risk awareness and privacy tool usage, as per Akoglu (2018). The value of • ranges from -1 to 1, with 0 indicating no association and ±1 indicating a perfect association. In this case, the positive value suggests that individuals who have heard of "digital privacy risks" are slightly more likely to use privacy-preserving smartphone tools. The approximate significance (p-value) for the • is < 0.001,

which is statistically significant. The Phi test suggests a strong association between privacy risk and privacy tool usage among the study participants. Where the awareness of privacy risk increases, privacy tool usage also increases.

Table 4.8 Phi test for Privacy Risk and Privacy Tools

Phi Test		Value	Approximate Significance
Nominal by Nominal	Phi	.182	<.001
N of Valid Cases		342	

For testing the significance between Privacy Risk and Security features, the questions Privacy Risk 1 (Have you heard of the term "digital privacy risks") and Security features (How familiar are you with the security features on your phone?) are considered for testing with Cramer's V correlation. Cramer's V is 0.125, which suggests a moderate association between familiarity with security features on smartphones and awareness of digital privacy risks, ($p = 0.068$), which means it is not significant that smartphone users who have heard of "digital privacy risks" are more likely to have checked their phone's security settings or changed default settings.

Table 4.9 Cramer's V Correlation for Privacy Risk and Security Features

		Value	Approximate Significance
Nominal by Nominal	Cramer's V	.125	**.068**
N of Valid Cases		342	

Therefore, from the conducted tests, smartphone users with a higher awareness of digital privacy risks are likelier to use privacy-enhancing tools but not security features and settings on their devices.

4.3.3 Hypothesis 3:

The third hypothesis stated, "The prevalence and type of privacy tools used differ significantly between iOS and Android smartphone users." For testing the hypothesis, the variable with iOS and Android is declared to test only for responses with either iOS marking as one or Android users marking as two and others marking as zero in IBM SPSS. Getting means would test the tools used for all iOS and Android users, but an ANOVA cannot be used as the variable is not continuous. Therefore, using Kruskal-Wallis test would be appropriate here. Kruskal-Wallis test was used for each of the privacy tools, starting from Encryption apps to Ad blockers were tested. The null hypothesis is chosen because the total tools used are the same across iOS vs. Android. From the results, it can be concluded that we retain the null hypothesis since there is no statistically significant difference in the distribution of the total number of tools used across the different smartphone operating systems. The result does not support the third hypothesis of the research.

Table 4.10 Kruskal-Wallis Test

Test	Sig.[a]
Kruskal-Wallis Test	0.338

a. The significance level is .050.

4.4 Analysis of privacy risks and reasons for privacy tools usage

The detailed analysis of digital privacy risks and the primary reason for privacy-preserving tools usage is explained in sections 4.4.1 and 4.4.2, respectively.

4.4.1 Digital Privacy Risks

The responses collected for the most significant privacy risk 324 out of 342 responded for biggest privacy risk, where 18 responses were left not responded by the users as this question in the survey was not required to be answered compulsorily. After analyzing the responses to the question "What would you consider to be the biggest digital privacy risks to you? Otherwise, type N/A, " a few responses stand out that provide insight into the variables affecting the usage of privacy tools on smartphones. Codes that emerged from content analysis for digital privacy risk concerns are given below in Table 4.11.

Table 4.11 Coding for Digital Privacy Risk Concern

Code	Definition	Example taken from user responses
Data Breach	Unauthorized access & retrieval of sensitive information.	Data breaches
Identity Access and Theft	Unauthorized use of personal information for fraudulent purposes.	Identity theft poses a serious threat.
Online Tracking and Profiling	Monitoring users' online activities to collect data and create user profiles.	Another significant risk is online tracking.
Weak Password & Authentication	Unauthorized access due to easily guessable passwords or inadequate authentication.	Reusing weak passwords.
Phishing Attacks	Fraudulent attempts to obtain sensitive information.	Phishing attacks are also a major concern.
Health Records	Unauthorized access to sensitive medical information.	Health Records

Most of the users provided more than one privacy risk, whereas 18 users provided only one privacy risk concern. The most concerned risk, with 44 responses, expressed concerns about data breaches, indicating worry about data breaches, which occur when sensitive personal information like names, addresses, financial details, and login credentials are exposed due to security measures, outdated software, or targeted malware attacks. The second most concerned one is access and theft, where 22 respondents emphasized the dangers of unauthorized access and theft of their personal information held by organizations, which could result in theft or manipulation of private information, including financial or medical health records (refer to Table 4.12).

Nine responses highlighted concerns regarding online tracking and profiling, including the risks associated with tracking, where companies track and gather data on users' browsing habits, personal beliefs, and purchasing behaviors without their consent. Avoiding tracking and profiling might lead individuals to embrace privacy tools that restrict data collection and sharing. Fourteen respondents were concerned about weak passwords and inadequate authentication, highlighted by participants as factors that expose information to risk. Being aware of these vulnerabilities could prompt users to utilize privacy tools that offer password management and extra layers of

authentication. Social engineering and phishing attacks were also considered threats to deceive individuals into disclosing sensitive data. Three respondents were concerned about phishing attacks leading the users to fall prey to tactics that could motivate users to employ privacy tools to identify and prevent these attacks on their mobile devices. 220 respondents answered N/A, where NA could state the user is not aware of privacy risks, and could be stated that the user was not concerned about privacy risks, leading this as a limitation (refer to Table 4.12).

The table below shows the most frequently provided responses. A few responses by the users were “Data breaches, phishing attacks” and “Data Breaches Unauthorized access to sensitive information stored by organizations can lead to data breaches.”, “Data Mining and Profiling”, “The starting point for identity theft can be publicly available information on social media”, “Health Records”. Tabe 4.12 lists the top digital privacy risk concerns stated by respondents. For the complete list, please see Appendix E.

Table 4.12 Digital Privacy Risk Concerns

Digital privacy risk concern	Frequency	Number of Users
Data Breach	46	44
Identity Access and Theft	22	22
Online Tracking and Profiling	9	9
Weak Password & Authentication	15	14
Phishing Attacks	3	3
Health Records	7	7
Responded N/A (not concerned about privacy)	220	220
Total		319

4.4.2 Primary reason for Privacy-Preserving tools usage

For the survey question “What is your primary reason for using privacy-preserving tools?” (see Appendix D), 327 respondents provided reasons out of 342 total responses, and the rest answered N/A. Though maximum responses revolved around personal information, the author came up with a few themes, such as maintaining control of personal information where the users have full authority over what personal information is shared, with whom, and for what purposes. Protection of personal data where the user focuses on protecting personal data from unauthorized

access, breaches, and cyber threats. Maintaining trust and confidence ensures that personal data is handled in a way that builds and maintains trust between the user and service providers. Preventing identity theft focuses on avoiding scenarios where personal information could be used fraudulently to impersonate the user. Users motivated by ensuring human dignity use privacy-preserving tools to protect their personal space ensuring their privacy. Refer Table 4.13 for coding, definition and example of response provided by the users.

Table 4.13 Coding for Primary reason for privacy tools usage

Code	Definition	Example of response provided by users
Maintaining control of personal information	The users have full authority over personal information that is shared.	Because it empowers me to maintain control over my personal information.
Protection of Personal data	The user focuses on protecting personal data from unauthorized access.	My primary reason for using privacy-preserving tools on my smartphone is to protect my personal information
Maintaining trust and confidence	The user ensures that personal data is handled with trust between the user and service providers.	Maintaining confidence and trust
Preventing Identity theft	The user focuses on avoiding scenarios where personal information could be used fraudulently.	Safeguarding against identity theft
Ensuring human dignity	The users use privacy-preserving tools to protect their personal space ensuring their privacy.	Ensuring human dignity

Seventy-four respondents stated their primary reason as maintaining control over their personal information and stressed the importance of privacy-preserving tools in empowering individuals to retain control over their data. By utilizing tools, individuals can dictate how their information is gathered, utilized, and shared, ensuring that their data remains protected from exploitation or misuse without explicit consent. The desire for autonomy and control over information significantly encourages people to embrace smartphone privacy-enhancing tools. Seventy-seven participants stated their reason for the Protection of Personal Data and mentioned

that safeguarding information was the primary reason for using privacy-preserving tools. These tools assist in securing data like financial details, medical records, private communications and other personally identifiable information (PII) against unauthorized access, misuse, or exposure. The imperative to safeguard data and prevent privacy breaches is a key driver for individuals opting to employ privacy-enhancing tools on their smartphones (refer to Table 4.14).

Maintaining trust and confidence was another reason that 16 respondents gave this reason. Respondents also underscored the significance of preserving privacy in fostering trust and confidence between individuals and organizations. With tools prioritizing privacy, people feel more confident in sharing their details with trusted sources, knowing their information will be treated responsibly and safeguarded from unauthorized access. This sense of trust plays a role in motivating people to embrace privacy focused tools on their smartphones. Preventing Identity theft and fraud was stated by 34 responders who followed this theme. One key reason for using privacy enhancing tools was the concern about identity theft, fraud and data misuse. By controlling who can access their information, individuals can reduce the risk of falling victim to such threats.

Ensuring human dignity, safety, and self-determination was another important aspect highlighted by some respondents, as well as the value of safeguarding dignity, safety, and self-determination through privacy protection. Privacy-centric tools empower individuals to uphold their privacy rights, express themselves freely, and maintain autonomy. This ethical viewpoint on privacy inspires certain individuals to incorporate privacy-enhancing features into their smartphone usage. The results indicate that the main factors impacting the use of smartphone privacy tools include wanting control over information, safeguarding sensitive data, building trust, preventing identity theft and fraud, and valuing privacy for dignity and self-determination. By focusing on these aspects, developers and companies can design privacy tools tailored to smartphone user's preferences. Quoting a few responses to support this, "ensuring human dignity" (for more detailed responses, refer to Appendix F).

A few responses by the users were "My primary reason for using privacy-preserving tools is to protect my personal", "Because it empowers me to maintain control over my personal information.", "maintaining confidence and trust", "Safeguarding against identity theft". Tabe 4.14 lists the top reasons given for usage of privacy-preserving tools. For the complete list, please see Appendix F.

Table 4.14 Primary reason for usage of privacy-preserving tools

Primary Reason	Number of Users
Maintaining Control on personal information	74
Protection of Personal data	77
Maintaining trust and confidence	16
Preventing Identity theft	34
Ensuring human dignity	8
Total	209

4.5 Summary

This chapter provided results for testing the hypothesis, understanding the biggest privacy risks and user's primary reasons for using privacy-preserving tools that helped answer the research question. The results show a significant difference in the use of privacy tools among smartphone users based on demographic factors such as age and familiarity with cybersecurity, supporting the first hypothesis. The results for the second hypothesis suggest that individuals aware of digital privacy risks are more likely to use privacy-preserving tools on their smartphones but do not use security features and settings present in the smartphones. The results did not support the third hypothesis. Most respondents stated data breaches as the most concerning privacy risk, followed by data theft, fraud, and online tracking and profiling. Most responders claimed the reason for using privacy-preserving tools was maintaining control of personal information, followed by protecting personal data and maintaining trust and confidence.

5. DISCUSSION

This study provided evidence supporting the first hypothesis that there is a significant difference in the use of privacy tools among smartphone users based on demographic factors such as age and familiarity with cybersecurity. Regarding the second hypothesis, this study supported that smartphone users with a higher awareness of digital privacy risks are likelier to use privacy-enhancing tools but need to be using settings and security features on their devices. Further, this study did not support the third hypothesis, which was mentioned as the prevalence and type of privacy tools used differ significantly between iOS and Android smartphone devices.

The results of this study supported the first hypothesis, “There is a significant difference in the use of privacy tools among smartphone users based on demographic factors such as age and familiarity with Cybersecurity”, which is consistent with the findings from other research papers. Nguyen et al. (2016) observed that individual user characteristics, including age, play a role in the value placed on smartphone privacy protection. This indicates that age is a demographic factor influencing how users perceive and prioritize smartphone privacy. Furini et al. (2020) analyzed users' privacy perceptions while using smartphone applications, highlighting the importance of understanding how different demographic groups view privacy in the smartphone context. This study implies that age and other demographic factors can influence how users interact with smartphone privacy features. Mamonov & Benbunan-Fich (2014) examined factors affecting perceptions of privacy breaches among smartphone application users, emphasizing the role of individual characteristics in shaping privacy concerns.

From the results for the second hypothesis, smartphone users aware of privacy risks tend to be more conscious about safeguarding their data by using privacy tools but are not using settings on their devices. Studies suggest that those with heightened concerns about privacy are more likely to take steps to protect their information and manage threats effectively (Huckvale et al., 2019). Educating smartphone users on privacy risks can encourage them to adopt tools and strategies that enhance device data protection (Crossler, 2019). However, there is a discrepancy between knowledge and beliefs regarding privacy, as individuals with knowledge may opt for less stringent privacy settings when they need more confidence in self-protection (Pal et al., 2020). Users who value control over their data are generally more alert to privacy risks, underscoring the significance of user awareness in shaping privacy behaviors and using measures (Lü & Li, 2022). However,

the results of this study suggest that smartphone users with higher awareness of digital privacy risks are more likely to use privacy-enhancing tools but not actually use security features and settings on their devices, which did not support the second hypothesis statement regarding settings and security features usage on smartphones by users.

The third hypothesis stated, "The prevalence and type of privacy tools used differ significantly between iOS and Android smartphone users," this study did not support the third hypothesis. Abrokwa et al., (2021) stated that they found no significant differences in privacy attitudes of different platform users of iOS and Android, which supports the result of the third hypothesis stating there is no significant difference in the usage of privacy tools among different smartphone platform users. Kollnig et al. (2021) state that although it has been suggested that smartphone architecture choices may safeguard user privacy, Kollnig's research does not show which operating system, iOS or Android is superior.

Although most respondents claimed to have carefully reviewed their smartphone's security settings, a significant number either stuck with default settings or only made changes when faced with specific issues. This discrepancy highlights a gap between user's privacy concerns and their actual security practices, emphasizing the importance of more proactive and comprehensive measures to safeguard personal devices. The responses this research got indicate that most of the responses are from the educated group and this is in line with several responses for people opting yes, no, I don't know these terminologies for the device being rooted or jailbroken survey question. Also, nearly three-fourths of the responders have been affected by a privacy breach, leading to why three-fourths of the responders have rooted or jailbroken their devices.

Out of the privacy tools listed, password managers are used by nearly 70% of the people, and next comes the usage of privacy focused browsers and antivirus software, followed by VPNs, Ad Blockers, and encryption apps. Out of respondents aware of digital privacy risks, nearly one-third of them were concerned about data breaches, theft of information, and phishing attacks, which is in line with the frequencies of responses that are very concerned about online privacy, personal information being misused, and personal information could be accessed by unknown parties. Based on the feedback received from the survey questions, it appears that people are inclined to use privacy-enhancing tools on their smartphones due to reasons like wanting control over their personal information, safeguarding sensitive data from unauthorized access, building

and maintaining trust concerns about identity theft and fraud and the belief that privacy is crucial for human safety.

By addressing these factors and motivations effectively, developers and organizations can develop smartphone privacy tools that meet users' requirements and preferences. Furthermore, the responses regarding the privacy risks indicate that users' awareness of digital privacy threats such as data breaches, unauthorized access, online tracking, weak passwords, and social engineering plays a significant role in their decision to adopt smartphone privacy-enhancing tools.

5.1 Limitations

The discussion reveals instances of participants copying and pasting identical responses from Internet searches rather than providing original answers. This raises data quality concerns and should be listed as a limitation. Similarly, the researchers note they cannot control or detect if respondents used search engines or AI tools like ChatGPT to generate free-form responses, which could also impact data authenticity. Future research could employ AI algorithms to detect patterns indicative of AI-generated or copied content. These algorithms can learn to recognize characteristics of non-original responses. The qualitative data was analyzed by a single person, the author, which might lead to bias. A second person could be used to code the same data to increase reliability of the results for future research. Some responses were irrelevant, suggesting hurried behavior by some participants rushing through the survey. These low-quality responses should be mentioned as a limitation. The sample skews heavily male (74.3%) and younger (56.1% aged 24-30), which may limit the generalizability of the findings to the broader population, and lead to bias. Future work could include a diverse range of demographics such as technology use. This helps in understanding how different groups perceive and use privacy tools.

The responses from the users for reason for usage of privacy-enhancing tools, seems to be pulled from other texts. For example, the response "Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII)" is taken from (AppsFlyer, n.d.). Using responses from previously existing work led to bias as the users are not providing their own reason. The over representation of Android users is another factor that could affect external validity. While the survey captures privacy perceptions and tool usage, it does not delve into the actual efficacy of these tools or the respondents' digital literacy in using them optimally. Despite

widespread tool use, the high breach incidence suggests potential gaps between privacy perceptions and actual protection.

5.2 Conclusion

This study helped to understand how prevalent the use of privacy-enhancing tools and settings among smartphone users is and helped understand the factors influencing their adoption and usage, answering the research question. The findings from this research are essential to understanding the motivation, reasons, and factors why smartphone users use privacy-enhancing tools. This research showed to what extent demographic factors, awareness levels, and smartphone platforms influence the adoption of privacy measures. The usage and adoption of default smartphone features and user privacy considerations can impact law enforcement interactions, as users' awareness and management of privacy settings influence data availability for investigative purposes. It is concluded that, in this era of smartphone usage, almost everyone is aware of privacy-enhancing tools. By investigating the prevalence of privacy tools and the factors influencing their adoption, law enforcement agencies can gain insights into potential privacy concerns and practices among smartphone users. This knowledge can be crucial in forensic investigations involving digital evidence from smartphones, where understanding the privacy settings and tools used by individuals can impact the collection and analysis of evidence.

Moreover, the hypotheses proposed in the study, such as the significant differences in privacy tool usage based on demographic factors and digital privacy awareness, can guide law enforcement in profiling and understanding user behavior related to privacy measures. Identifying that users with higher awareness of digital privacy risks are more likely to use privacy tools can help law enforcement anticipate the privacy measures taken by different user groups during investigations. The hypothesis suggests that differences in the types of privacy tools used by iOS and Android users can be valuable for forensic investigators dealing with devices running different operating systems. Understanding these platform-specific trends in privacy tool adoption can inform digital forensic strategies tailored to each operating system, enhancing the efficiency and accuracy of investigations involving iOS and Android devices.

These findings indicate that users' understanding of digital privacy risks, including data breaches, unauthorized access, online tracking, weak passwords, and social engineering, greatly influences their choice to adopt and utilize privacy-enhancing smartphone tools. By recognizing

these risk elements, developers can design privacy tools that directly tackle users' worries while providing them with the necessary protection and control over their personal information. The discovery that three-quarters of respondents had encountered a data breach is alarming and emphasizes the prevalence of digital privacy threats.

Data breaches and privacy risks have increased in recent years, impacting various sectors. The Verizon Data Breach Investigations Report (DBIR) is a valuable resource that provides insights into cyber security trends and developments ("Verizon: 2019 Data Breach Investigations Report", 2019). Collaborating with security firms, law enforcement agencies, and government bodies, the report sheds light on the landscape of data breaches. Implementing regulations such as the HIPAA Omnibus Rules has reduced the frequency of medical data breaches (Yaraghi & Gopal, 2018). While the survey didn't delve into the specifics of these breaches, the high occurrence rate suggests that vulnerabilities persist among individuals who are relatively mindful of privacy issues.

Further research could delve deeper into these breaches' circumstances and how users responded to them. Another aspect worth exploring is how demographic factors relate to attitudes and behaviors around privacy. Although this survey didn't specifically address these connections, previous studies have indicated that age, gender, and other personal characteristics can influence how people approach privacy. The survey findings also raise concerns regarding the efficacy of privacy protection methods and the obstacles to implementing stronger measures. Although most participants mentioned using some privacy tools, it remains uncertain whether they are utilized effectively and consistently. Moreover, the prevalence of users sticking to default security settings hints at usability or accessibility issues hindering broader adoption of best practices. It is crucial for researchers, tech companies, and policymakers to overcome these barriers.

REFERENCES

Abrokwa, D., Das, S., Akgul, O., & Mazurek, M. L. (2021). Comparing Security and Privacy Attitudes Among {US}. Users of Different Smartphone and {Smart-Speaker} Platforms. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (pp. 139-158).

Abu Bakar, A., Mahinderjit Singh, M., & Mohd Shariff, A. R. (2021). A privacy preservation quality of service (Qos) model for data exposure in android smartphone usage. *Sensors*, *21*(5), 1667. 5445.

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, *29*, 701-750.

Akoglu, H. (2018). User's guide to correlation coefficients. *Turkish journal of emergency medicine*, *18*(3), 91-93.

Alani, M. M. (2017). Android users privacy awareness survey. *International Journal of Interactive Mobile Technologies*, *11*(3).

Alashi, S. A., & Aldahawi, H. A. (2020). Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their Use in the Kingdom of Saudi Arabia. *Journal of Information Security and Cybercrimes Research*, *3*(1), 31-57.

Alendal, G., Dyrkolbotn, G. O., & Axelsson, S. (2021). Digital forensic acquisition kill chain–analysis and demonstration. In *Advances in Digital Forensics XVII: 17th IFIP WG 11.9 International Conference, Virtual Event, February 1–2, 2021, Revised Selected Papers 17* (pp. 3-19). Springer International Publishing.

Alghamdi, M. I. (2021). Digital forensics in cyber security—recent trends, threats, and opportunities. *Cybersecurity Threats with New Perspectives*.

Alkahtani, H., & Aldhyani, T. H. (2022). Artificial intelligence algorithms for malware detection in android-operated mobile devices. *Sensors*, *22*(6), 2268.

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS one*, *12*(3), e0173284.

Anggraeny, I., Monique, C., Wardoyo, Y. P., & Slamet, A. B. (2022). The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department. *KnE Social Sciences*, 349-359.

AppsFlyer. (n.d.). Privacy preserving technologies. AppsFlyer. Retrieved June 19, 2024, from https://www.appsflyer.com/glossary/privacy-preserving-technologies/

Ayres-Pereira, V., Pirrone, A., Korbmacher, M., Tjostheim, I., & Böhm, G. (2022). The privacy and control paradoxes in the context of smartphone apps. *Frontiers in Computer Science*, *4*, 986138.

Azad, M. A., Arshad, J., Akmal, S. M. A., Riaz, F., Abdullah, S., Imran, M., & Ahmad, F. (2020). A first look at privacy analysis of COVID-19 contact-tracing mobile applications. *IEEE internet of things journal*, *8*(21), 15796-15806.

Barth, S. (2021). Data, data, and even more data: Empowering users to make well-informed decisions about online privacy.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 1017-1041.

Belkhamza, Z., Niasin, M. A. F., & Idris, S. (2019). The effect of privacy concerns on the purchasing behavior among Malaysian smartphone users. In *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications* (pp. 1154-1170). IGI Global.

Benthall, S., Hatna, E., Epstein, J. M., & Strandburg, K. J. (2022). Privacy and contact tracing efficacy. *Journal of the Royal Society Interface*, *19*(194), 20220369.

Bracamonte, V., Pape, S., & Loebner, S. (2022). "All apps do this": Comparing Privacy Concerns Towards Privacy Tools and Non-Privacy Tools for Social Media Content. *Proceedings on Privacy Enhancing Technologies*.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers & Security*, *88*, 101647.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data?. *Perspectives on psychological science*, *6*(1), 3-5.

Burnham, M. J., Le, Y. K., & Piedmont, R. L. (2018). Who is Mturk? Personal characteristics and sample consistency of these online workers. *Mental Health, Religion & Culture*, *21*(9-10), 934-944.

Carelli, A., Sinclair, M., & Southee, D. (2019). Short paper: initial recommendations for the design of privacy management tools for smartphones. In *Human-Computer Interaction–INTERACT 2019: 17th IFIP TC 13 International Conference, Paphos, Cyprus, September 2–6, 2019, Proceedings, Part III 17* (pp. 486-496). Springer International Publishing.

Carter, S. E. (2022). A value-centered exploration of data privacy and personalized privacy assistants. *Digital Society*, *1*(3), 27.

Chandler, J., Rosenzweig, C., Moss, A. J., Robinson, J., & Litman, L. (2019). Online panels in social science research: Expanding sampling methods beyond Mechanical Turk. *Behavior research methods*, *51*, 2022-2038.

Chatterjee, S., Chaudhuri, R., Vrontis, D., & Hussain, Z. (2021). Usage of smartphone for financial transactions: from the consumer privacy perspectiv

Cheng, Z., Li, K., & Teng, C. I. (2022). Understanding the influence of privacy protection functions on continuance usage of push notification service. *Aslib Journal of Information Management*, *74*(2), 202-224.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-16). e. *Journal of Consumer Marketing*, *40*(2), 193-208.

Chittaranjan, G., Blom, J., & Gatica-Perez, D. (2013). Mining large-scale smartphone data for personality studies. *Personal and Ubiquitous Computing*, *17*, 433-450.

Crossler, R. E., & Bélanger, F. (2019). Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research*, *30*(3), 995-1006.

Dixon, M., Sillence, E., Nicholson, J., & Coventry, L. (2023, October). "It's the one thing that makes my life tick": Security Perspectives of the Smartphone Era. In *Proceedings of the 2023 European Symposium on Usable Security* (pp. 97-111).

Dogruel, L., Joeckel, S., & Henke, J. (2023). Disclosing personal information in mhealth apps. Testing the role of privacy attitudes, app habits, and social norm cues. *Social Science Computer Review*, *41*(5), 1791-1810.

Duan, S. X., & Deng, H. (2022). Exploring privacy paradox in contact tracing apps adoption. *Internet Research*, *32*(5), 1725-1750.

Elo S, Kyngas H. The qualitative content analysis process. *J Adv Nurs* 2008; 62(1): 107–115.

Faurholt-Jepsen, M., Busk, J., Frost, M., Vinberg, M., Christensen, E. M., Winther, O., ... & Kessing, L. V. (2016). Voice analysis as an objective state marker in bipolar disorder. *Translational psychiatry*, *6*(7), e856-e856.

Feng, Y., Chen, L., Zheng, A., Gao, C., & Zheng, Z. (2019). AC-Net: Assessing the consistency of description and permission in Android apps. *IEEE Access*, *7*, 57829-57842.

Forkus, S. R., Contractor, A. A., Goncharenko, S., Goldstein, S. C., & Weiss, N. H. (2022). Online crowdsourcing to study trauma and mental health symptoms in military populations: A case for Amazon's Mechanical Turk (MTurk) platform. *Psychological trauma: theory, research, practice, and policy*.

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy perception when using smartphone applications. *Mobile Networks and Applications*, *25*, 1055-1061.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *digital investigation*, *7*, S64-S73.

Gerdon, F., Nissenbaum, H., Bach, R. L., Kreuter, F., & Zins, S. (2020). Individual acceptance of using health data for private and public benefit: Changes during the COVID-19 pandemic. *Harvard Data Science Review*.

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. *Nurse education today*, *24*(2), 105-112.

Grande, D., Luna Marti, X., Merchant, R. M., Asch, D. A., Dolan, A., Sharma, M., & Cannuscio, C. C. (2021). Consumer views on health applications of consumer digital data and health privacy among US adults: qualitative interview study. *Journal of Medical Internet Research*, *23*(6), e29395.

Halboob, W., & Almuhtadi, J. (2023). Computer Forensics Framework for Efficient and Lawful Privacy-Preserved Investigation. *Computer Systems Science & Engineering*, *45*(2).

Harborth, D., Hatamian, M., Tesfay, W. B., & Rannenberg, K. (2019). *A two-pillar approach to analyze the privacy policies and resource access behaviors of mobile augmented reality applications* (pp. 5029-5038). University of Hawai'i Press.

Hatamian, M. (2020). Engineering privacy in smartphone apps: A technical guideline catalog for app developers. *IEEE Access*, *8*, 35429-3

Hsieh, J. K., & Li, H. T. (2022). Exploring the fit between mobile application service and application privacy. *Journal of Services Marketing*, *36*(2), 264-282.

Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA network open*, *2*(4), e192542-e192542.

Ieong, R. S. (2006). FORZA–Digital forensics investigation framework that incorporate legal issues. *digital investigation*, *3*, 29-36.

Jabali, O., Saeedi, M., Shbeitah, G., & Ayyoub, A. A. (2019). Medical faculty members' perception of smartphones as an educational tool. *BMC medical education*, *19*, 1-9.

Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of forensic sciences*, *60*(4), 885-893.

Kim, H. S., & Hodgins, D. C. (2017). Reliability and validity of data obtained from alcohol, cannabis, and gambling populations on Amazon's Mechanical Turk. *Psychology of addictive behaviors*, *31*(1), 85.

Knijnenburg, B. P., Anaraky, R. G., Wilkinson, D., Namara, M., He, Y., Cherry, D., & Ash, E. (2022). User-Tailored Privacy.

Kollnig, K., Shuba, A., Binns, R., Van Kleek, M., & Shadbolt, N. (2021). Are iphones really better for privacy? comparative study of ios and android apps. *arXiv preprint arXiv:2109.13722*.

Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., & Shadbolt, N. (2022, June). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 508-520).

Kovanič, M., & Spáč, S. (2022). Conceptions of privacy in the digital era: Perceptions of slovak citizens. *Surveillance & Society*, *20*(2), 186-201.

Kulyk, O., Gerber, P., Marky, K., Beckmann, C., & Volkamer, M. (2019). Does this app respect my privacy? Design and evaluation of information materials supporting privacy-related decisions of smartphone users. In *Workshop on usable security (USEC'19). San Diego, CA* (pp. 1-10).

Levay, K. E., Freese, J., & Druckman, J. N. (2016). The demographic and political composition of Mechanical Turk samples. *Sage Open*, *6*(1), 2158244016636433.

Lu, Y., & Li, S. (2022). From data flows to privacy-benefit trade-offs: A user-centric semantic model. *Security and Privacy*, *5*(4), e225.

Lyon, G. (2023). Informational inequality: the role of resources and attributes in information security awareness. *Information & Computer Security*.

Maceli, M. G. (2018). Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries. *IFLA journal*, *44*(3), 195-202.

Mamonov, S., & Benbunan-Fich, R. (2014, January). Factors affecting perceptions of privacy breach among smartphone application users. In *2014 47th Hawaii International Conference on System Sciences* (pp. 3178-3187). IEEE.

Maseeh, H. I., Nahar, S., Jebarajakirthy, C., Ross, M., Arli, D., Das, M., ... & Ashraf, H. A. (2023). Exploring the privacy concerns of smartphone app users: A qualitative approach. *Marketing Intelligence & Planning*, *41*(7), 945-969.

Mavroeidi, A. G., Kitsiou, A., & Kalloniatis, C. (2020). The role of gamification in privacy protection and user engagement. *Security and Privacy from a Legal, Ethical, and Technical Perspective*, 132-166.

Meier, Y., Meinert, J., & Krämer, N. C. (2021). Investigating factors that affect the adoption of COVID-19 contact-tracing apps: A privacy calculus perspective.

Meier, Y., Schäwel, J., & Krämer, N. C. (2021). Between protection and disclosure: applying the privacy calculus to investigate the intended use of privacy-protecting tools and self-disclosure on different websites. *SCM Studies in Communication and Media*, *10*(3), 283-306.

Mellis, A. M., & Bickel, W. K. (2020). Mechanical Turk data collection in addiction research: Utility, concerns and best practices. *Addiction*, *115*(10), 1960-1968.

Montasari, R. (2017). A standardised data acquisition process model for digital forensic investigations. *International Journal of Information and Computer Security*, *9*(3), 229-249.

Morosan, C. (2014). Toward an integrated model of adoption of mobile phones for purchasing ancillary services in air travel. *International journal of contemporary hospitality management*, *26*(2), 246-271.

Mosa, A. S. M., Yoo, I., & Sheets, L. (2012). A systematic review of healthcare applications for smartphones. *BMC medical informatics and decision making*, *12*, 1-31.

Mosenia, A., Dai, X., Mittal, P., & Jha, N. K. (2017). Pinme: Tracking a smartphone user around the world. *IEEE Transactions on Multi-Scale Computing Systems*, *4*(3), 420-435.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.

Nettrour, J. F., Burch, M. B., & Bal, B. S. (2019). Patients, pictures, and privacy: managing clinical photographs in the smartphone era. *Arthroplasty today*, *5*(1), 57-60.

Nguyen, K. D., Rosoff, H., & John, R. S. (2016). The effects of attacker identity and individual user characteristics on the value of information privacy. *Computers in Human Behavior*, *55*, 372-383.

Obidzinski, M., & Oytana, Y. (2018). Presumption of innocence and deterrence.

Ohme, J., Araujo, T., de Vreese, C. H., & Piotrowski, J. T. (2021). Mobile data donations: Assessing self-report accuracy and sample biases with the iOS Screen Time function. *Mobile Media & Communication*, *9*(2), 293-313.

Padyab, A., Päivärinta, T., Ståhlbröst, A., & Bergvall-Kåreborn, B. (2019). Awareness of indirect information disclosure on social network sites. *Social Media+ Society*, *5*(2), 2056305118824199.

Pal, D., Arpnikanondt, C., & Razzaque, M. A. (2020). Personal information disclosure via voice assistants: the personalization–privacy paradox. *SN Computer Science*, *1*, 1-17.

Panova, O. O., Tanko, A. V., Povydysh, V. V., & Alieksieieva, O. V. (2020). Law enforcement agencies in the system of entities of protection and defense of human rights.

Patel, A., & Palomar, E. (2016, July). LP-Caché: Privacy-aware cache model for location-based apps. In *International Conference on Security and Cryptography* (Vol. 2, pp. 183-194). SCITEPRESS.

Paul, S. K. (2022). Sok: is iphone actually secure?. International Journal of Advanced Research, 10(04), 743-746. https://doi.org/10.21474/ijar01/14609

Pourvahab, M., & Ekbatanifard, G. (2019). Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. *IEEE Access*, *7*, 153349-153364.

Pratama, A. R., Firmansyah, F. M., & Rahma, F. (2022). Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality. *PeerJ Computer Science*, *8*, e918.

Prince, C., Omrani, N., & Schiavone, F. (2024). Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. *Information Technology & People*, *37*(8), 1-24.

Ramadhan, R. A., Setiawan, P. R., & Hariyadi, D. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037: 2012 and NIST SP800-86 Framework. *IT Journal Research and Development*, *6*(2), 162-168.

Ramokapane, K. M., Mazeli, A. C., & Rashid, A. (2023). Skip, skip, skip, accept!!!: A study on the usability of smartphone manufacturer provided default features and user privacy. *arXiv preprint arXiv:2308.14593*.

Reinfelder, L., Benenson, Z., & Gassmann, F. (2014). Differences between Android and iPhone users in their security and privacy awareness. In *Trust, Privacy, and Security in Digital Business: 11th International Conference, TrustBus 2014, Munich, Germany, September 2-3, 2014. Proceedings 11* (pp. 156-167). Springer International Publishing.

Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., & Dwivedi, Y. K. (2020). Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps. *IEEE Transactions on Engineering Management*.

Sharma, T., & Bashir, M. (2020). Are PETs (Privacy Enhancing Technologies) Giving Protection for Smartphones?--A Case Study. *arXiv preprint arXiv:2007.04444*.

Shaw Jr, G., Nadkarni, D., Phann, E., Sielaty, R., Ledenyi, M., Abnowf, R., ... & Chen, S. (2022). Separating features from functionality in vaccination apps: computational analysis. *JMIR Formative Research*, *6*(10), e36818.

Sheng, H., Nah, F. F. H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, *9*(6), 1.

Shuijing, H., & Tao, J. (2017, October). An empirical study on digital privacy risk of senior citizens. In *2017 International Conference on Robots & Intelligent System (ICRIS)* (pp. 19-24). IEEE.

Sibe, R. T., & Muller, S. R. (2022). Digital forensic readiness of cybercrime investigating institutions in nigeria: a case study of the Economic and Financial Crimes Commission (EFCC) and the Nigeria police force. *Annals of Computer Science and Information Systems*, *34*.

Skalkos, A., Stylios, I., Karyda, M., & Kokolakis, S. (2021). Users' privacy attitudes towards the use of behavioral biometrics continuous authentication (BBCA) technologies: A protection motivation theory approach. *Journal of Cybersecurity and Privacy*, *1*(4), 743-766.

Smernytskyi, D., Zaichko, K., Zhvanko, Y., Bakal, M., & Shapochka, T. (2021). Comparative analysis of the legislative support for law enforcement agencies in the post-soviet space and Europe. *Cuestiones Políticas*, *39*(70).

Snir, J. T., Ko, D. N., Pratt, B., & McDougall, R. (2022). Anticipated impacts of voluntary assisted dying legislation on nursing practice. *Nursing ethics*, *29*(6), 1386-1400.

Stamm, M. C., & Liu, K. R. (2011). Anti-forensics of digital image compression. *IEEE Transactions on Information Forensics and Security*, *6*(3), 1050-1065.

Story, P., Smullen, D., Yao, Y., Acquisti, A., Cranor, L. F., Sadeh, N., & Schaub, F. (2021). Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

Sudirman, B. P., & Sari, P. K. (2023). Differences in Information Security Behavior of Smartphone Users in Indonesia Using Pearson's Chi-square and Post Hoc Test. *International Journal on Advanced Science, Engineering & Information Technology*, *13*(2).

Tahaei, M., Li, T., & Vaniea, K. (2022). Understanding privacy-related advice on stack overflow. *Proceedings on Privacy Enhancing Technologies*.

Tahaei, M., Vaniea, K., & Saphra, N. (2020, April). Understanding privacy-related questions on stack overflow. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1-14).

Torous, J., & Haim, A. (2018). Dichotomies in the development and implementation of digital mental health tools. *Psychiatric Services*, *69*(12), 1204-1206.

Tovino, S. A. (2020). Privacy and security issues with mobile health research applications. *The Journal of Law, Medicine & Ethics*, *48*(1_suppl), 154-158.

Tran, K., Morra, D., Lo, V., Quan, S., & Wu, R. (2014). *The use of smartphones on General Internal Medicine wards: a mixed methods study. Appl Clin Inform, 5 (3), 814-823. doi: 10.4338*. ACI-2014-02-RA-0011.

Tsetsi, E., & Rains, S. A. (2017). Smartphone Internet access and use: Extending the digital divide and usage gap. *Mobile Media & Communication*, *5*(3), 239-255.

Ubhi, H. K., Kotz, D., Michie, S., Van Schayck, O. C., & West, R. (2017). A comparison of the characteristics of iOS and Android users of a smoking cessation app. *Translational behavioral medicine*, *7*(2), 166-171.

Ullah, S., Khan, M. S., Lee, C., & Hanif, M. (2022). Understanding users' behavior towards applications privacy policies. *Electronics*, *11*(2), 246.

Utz, C., Becker, S., Schnitzler, T., Farke, F. M., Herbert, F., Schaewitz, L., ... & Dürmuth, M. (2021, May). Apps against the spread: Privacy implications and user acceptance of COVID-19-related smartphone apps on three continents. In *Proceedings of the 2021 chi conference on human factors in computing systems* (pp. 1-22).

Wang, W., & Zhang, Q. (2014, April). A stochastic game for privacy preserving context sensing on mobile phone. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications* (pp. 2328-2336). IEEE.

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science*, *1*(1), 3-20.

Wettlaufer, J., & Simo, H. (2020). Decision support for mobile app selection via automated privacy assessment. *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14*, 292-307.

Wolff, M. S., & Niessen, C. (2023). Everything under control? The impact of electronic monitoring type and social norms on privacy and reactance. *Journal of Personnel Psychology*.

Yan, K., Shen, W., Jin, Q., & Lu, H. (2019). Emerging privacy issues and solutions in cyber-enabled sharing services: From multiple perspectives. *IEEE Access*, *7*, 26031-26059.

Yen, T. F. (2022). Digital Risk, Digital Privacy and their Impacts on the Usage Intentions of Smart Senior Health Care Service. *International Journal of Social Sciences Perspectives*, *11*(2), 105-113.

Yudhana, A., Riadi, I., & Anshori, I. (2018). Identification of Digital Evidence Facebook Messenger on Mobile Phone With National Institute of Standards Technology (Nist) Method. *Jurnal Ilmiah Kursor*, *9*(3).

Zhang, L., Li, Y., Wang, L., Lu, J., Li, P., & Wang, X. (2017). An efficient context-aware privacy preserving approach for smartphones. *Security and Communication Networks*, *2017*.

Zhang, M., Chow, A., & Smith, H. (2020). COVID-19 contact-tracing apps: analysis of the readability of privacy policies. *Journal of Medical Internet Research*, *22*(12), e21572.

Zhang, Y., Barbara M. Wildemuth,(2005)," Qualitative Analysis of Content. *Human Brain Mapping*, *30*(7), 2197-2206.

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, *111*(2), 212-226.

Zhou, Y., Piekarska, M., Raake, A., Xu, T., Wu, X., & Dong, B. (2017). Control yourself: on user control of privacy settings using personalization and privacy panel on smartphones. *Procedia Computer Science*, *109*, 100-107.

Zimmeck, S., Wang, O., Alicki, K., Wang, J., & Eng, S. (2023). Usability and enforceability of global privacy control. *Proceedings on Privacy Enhancing Technologies*.

Zou, Q., Wang, Y., Wang, Q., Zhao, Y., & Li, Q. (2020). Deep learning-based gait recognition using smartphones in the wild. *IEEE Transactions on Information Forensics and Security*, *15*, 3197-3212.

APPENDIX A. IRB EXEMPTION

IRB-2024-326 - Initial: 1. EXEMPTION MEMO

PURDUE UNIVERSITY

This Memo is Generated From the Purdue University Human Research Protection Program System, Cayuse IRB.

Date: March 4, 2024
PI: MARCUS ROGERS
Re: Initial - IRB-2024-326 *Attitude towards Privacy Preserving Tools on Smartphones*

The Purdue University Human Research Protection Program (HRPP) has determined that the research project identified above qualifies as exempt from IRB review, under federal human subjects research regulations 45 CFR 46.104. The Category for this Exemption is listed below . Protocols exempted by the Purdue HRPP do not require regular renewal. However, the administrative check-in date is March 3, 2027. The IRB must be notified when this study is closed. If a study closure request has not been initiated by this date, the HRPP will request study status update for the record.

Specific notes related to your study are found below.
Decision: Exempt
Category: Category 2.(i). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:
The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects;
Category 2.(ii). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:
Any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation; or

Any modifications to the approved study must be submitted for review through Cayuse IRB. All approval letters and study documents are located within the Study Details in Cayuse IRB.

APPENDIX B. IRB NARRATIVE

Intervention And Data Collection Method

We have a consent form that respondents will have to agree to before starting the survey. The study will implement a comprehensive data collection method via Amazon MTurk, leveraging an anonymous payment system to incentivize participation. Utilizing Qualtrics for hosting the survey, participants will be systematically screened to ensure eligibility, focusing on age, residency, and employment status within the U.S. The quantitative research employed validated instruments to measure insider threat traits, cyberaggressiveness, and social support, incorporating attention-check questions and reCAPTCHA to enhance data integrity. This methodological approach aims to explore the nexus between external cyberaggression, the absence of social support, and the genesis of insider threats in corporate environment. The study will uphold respondent autonomy by allowing participants the option to decline answering any questions within the Cyber Crime Index, Cyberbullying Experiences Survey, and the online/offline social support scales. This safeguard will be implemented to respect participant comfort and consent, contributing to the integrity and inclusiveness of the research findings.

Payment Or Incentive

Respondents will be anonymously paid through an anonymous payment system set up by Amazon's MTurk. After the questionnaire, a final page is presented that thanks the participant and instructs them to please use the following code words to receive payment: Go Purdue! A respondent would then return to the MTurk solicitation page and enter Go Purdue into the text box. The researcher would then be notified, via email, that a respondent completed the survey. If the respondent enters the correct code words, the researcher will pay them through the anonymous account. Each participant will be paid $0.75 for completing the study. Funds allotted for paying participants for survey completion will be disbursed from the Department of Computer and Information Technology at Purdue University. The study aims to recruit 350 respondents from Amazon MTurk. No identifying information will be collected; this survey will be completely anonymous.

Study Procedures

This research aims to explore behaviors around privacy preserving technologies. The research team will conduct the research study using quantitative and qualitative survey methods. The research survey will be hosted on Qualtrics, and participants will be recruited from Amazon MTurk. The survey consists of a questionnaire and see attached. Participants will be asked to provide some of their demographic information followed by responses to the questionnaire around privacy preserving technologies. Respondents will be solicited automatically by Amazon MTurk given our inclusion criteria.

This solicitation Thesis_Survey_Attitude_Towards_Privacy_preserving_tools_on_ Smartphones.docx will include a survey link that respondents can click on if they are interested in participating. This link will direct them to Purdue University's Qualtrics website, where the entirety of the study procedures will take place. The opening page of the Qualtrics survey will include the Informed Consent (see Attachment: Informed Consent). If respondents choose to proceed with participation, they will click on the survey link and be directed to the survey. There will be no direct or indirect contact between researchers and potential participants. No identifying information will be collected. Only individuals 18 years of age older AND who currently reside in the United States will be eligible to complete the study. Following this, participants will be presented with a questionnaire measuring privacy preserving technology use. In addition, the survey will also employ ReCAPTCHA and Embedded data will be used within Qualtrics to prevent the automated responses from bots.

Study Instruments And Questionnaires

There are a total of 16 questions. The first two questions are demographics on age and gender, another demographic question related to cybersecurity knowledge and a question on familiarity with security features are taken from Breitinger, F., & Hassenfeldt, C. (2020). Privacy concern questions are taken from Skalkos, A et al., (2021) and provided likert scale where 1- Not Concerned at all to 5- Strongly Concerned. Options for privacy tools questions are taken from Story. P et al., (2021) and Dixon. M et al., (2023). Smartphone OS and device questions are taken from the reference Abrokwa, D. et al., (2021). Data privacy and Privacy risk yes/no questions are added to know knowledge on privacy risks. Knowing about the prevalence of the usage of privacy-preserving tools based on demographic factors helps my study. The study

helps understand smartphone OS and attitudes towards what kind of privacy tools are being used. The research team will conduct a study on awareness of cybersecurity and privacy risks with the usage of privacy tools. Once the research team gets the responses, statistical analysis will be used to bring out the required results. Attaching the survey questions below.

APPENDIX C. IRB RECRUITMENT

MTurk Solicitation

MTurk requires certain fields to be filled in and are restricted by character count. The current study will include the following information based on MTurk's standard solicitation page:

- **Title**: Anonymous survey: Attitude towards Privacy preserving tools on smartphones
- **Brief Description**: Give us your anonymous opinion on different comments posted anonymously online (approximately 5 – 7 minute survey).
- **Keywords**: Anonymous survey, Privacy preserving tools.
- **Reward per assignment**: 0.75$
- **Qualifications Required**: 18 years of age or older, US permanent residents.

Anonymous survey: Attitudes Toward Privacy preserving tools on smartphones

You have the opportunity to be a part of research! Researchers are conducting an anonymous study on people's attitudes towards Privacy preserving tools on smartphones.
The study involves a short, anonymous survey. It will take approximately 5 - 7 minutes to complete. We will not be collecting any identifiable information (e.g., your name, IP address). Instead, your responses to the survey will be coded with a random "ID number" so we will not have to ask you for any personal information. This HIT is periodically reposted; so, if you have already completed this HIT previously, please do not complete it a second time. You will not be compensated a second time.

Anonymous Survey link: qualtrics.purdue.edu

In order to be compensated for completing this survey, please enter the survey code here:

Thank You Web Page (Final Page of Study)

*Final page for those who successfully completed study

Thank You!

We appreciate you taking the time to be a part of research.

If you have any questions about this survey, you may contact rogersmk@purdue.edu , the Principal Investigator at or refer to **IRB-2024-326**

In order to receive compensation, please enter the following code into MTurk: " **GoPurdue!** ".

"Sorry Page"

*Last page for respondents declined consent or screened out of survey because under 18 years of age or who are not living in the United States.

Sorry, but based on one or more of your responses, you did not qualify for this study.

Thank you for your interest, and please contact the Principal Investigator if you have any questions: Dr. Marcus Rogers (rogersmk@purdue.edu) or refer to **IRB-2024-326**

APPENDIX D. RESEARCH SURVEY

Consent Form

IRB-2024-326

RESEARCH PARTICIPANT INFORMATION FORM

"Attitudes towards privacy-preserving tools on smartphones"

Principle Investigator: Dr. Marcus Rogers

IRB Number: **IRB-2024-326**

Computer & Information Technology

Purdue University

Key Information:

You are being asked to participate or be a part of a research study. Your participation is voluntary which means that you may choose not to participate at any time. Please read this form and ask any questions before you agree to be in the study. If you decide to take part in the study, you will be asked to sign this form. Be sure you understand what you will do and any possible risks or benefits.

The researchers hope to learn about attitudes towards usage of privacy preserving tools on smartphones. This study is only intended for people who are 18 years of age or older and who are living in the united States only. **Do not complete the study if you are not legally considered an adult.**

What will I do if I choose to be in this study?

An anonymous, online survey will be administered using a secure website. Once you have read this consent form, and agree to voluntarily participate, you will be taken to the anonymous, online survey. You may withdraw from the survey at any time, and you may skip or decline any questions that you do not wish to answer. **How long will I be studying?**

We expect that the one-time survey will take about 5 - 7 minutes to complete. The anonymous data will be kept for approximately 5 months.

What are the possible risks or discomforts?

The risks of taking this survey are similar to those experienced in everyday life. Please know that this is an anonymous survey, and we will not be able to link your responses back to you. We do not ask for any identifiable information (e.g., Name, email). Breach of confidentiality is always a risk with data, but we will take precautions to minimize this risk as described in the confidentiality section.

Are there any potential benefits?

It is unlikely that there will be direct benefits to you from participating. Having more information from the answers in this research study might help us understand more about individual's attitudes towards the workplace environment. Eventually, we hope to publish the research results, and if you want to see them, you should send an email requesting information to the Principal Investigator at rogersmk@purdue.edu .

Will I receive payment or other incentive?

You will receive compensation for your participation in the study. Each participant will be paid $0.75 for completing the study. Respondents will be anonymously paid Amazon's MTurk. After the questionnaire, a final page is presented that thanks the participant and instructs them to please use the given code words to receive payment at the end of the survey. The researcher would then be notified, via email, that a respondent completed the survey. If the respondent enters the correct code words, the researcher will pay them through the anonymous account.

Will information about me and my participation be kept confidential?

The project's research records may be reviewed by departments at Purdue University responsible for regulatory and research oversight. We do not ask for your name or any other information that could be used to identify you at any time before, during, or after the survey. While demographics information is collected, the questions are broad enough to prevent reidentification of your data through this information. No IP addresses will be recorded. There will be no way to determine

where the survey was taken or by whom. Instead, the survey software will randomly assign an ID number to your responses. This means that the responses to the questionnaires cannot be linked or matched to you, which means your responses will remain completely anonymous. Only researchers associated with this study will have access to the anonymous data.

What are my rights if I take part in this study?

You do not have to participate in this research project. If you agree to participate, you may withdraw your participation at any time without penalty or loss of benefits to which you are otherwise entitled.

Who can I contact if I have questions about the study?

If you have questions, comments, or concerns about this research project, you can talk to one of the researchers. Please contact the Principal Investigator at rogersmk@purdue.edu .

If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write to: Human Research Protection Program - Purdue University Ernest C. Young Hall, Room 1010 155 S. Grant St. West Lafayette, IN 47907-2114. To report anonymously via Purdue's Hotline, see www.purdue.edu/hotline.

By clicking this box, I agree to take part in this survey. I am 18 years of age or older and understand the information above about my participation.

Consent Response

- o I Agree (1)
- o I Do Not Agree (2)

End of Block: Consent

Start of Block: Label Captcha

Before you proceed to the survey, please complete the captcha below.

End of Block: Label Captcha

Start of Block: Demographics

Age: What is your age group?

- o Under 18 (1)
- o 18 - 23 (2)
- o 24 - 30 (3)
- o 31 - 40 (4)
- o 41 - 50 (5)
- o 51 - 60 (6)
- o Over 60 (7)
- o Prefer not to say (8)

Gender: What is your gender identity?

- o Male (1)
- o Female (2)
- o Non-binary / third gender (3)
- o Prefer not to say (4)

End of Block: Demographics

Start of Block: Privacy Tools Usage

Smartphone OS: What operating system do you have on your smartphone?

- o iOS (1)
- o Android (2)
- o I do not have a smart phone (3)
- o I use both iOS and Android (4)
- o Other (5)

Familiarity: How familiar are you with cybersecurity (on a scale of 1–5)?

- o 1 - I have no knowledge of related topics (1)
- o 2 - I follow the news of related topics (2)
- o 3 - I have read/taught myself about related topics (3)
- o 4 - I have taken one or more courses in a related topic or have a certification (4)
- o 5 - I have a degree in this or a related field (5)

Data Privacy: Have you ever been effected by a data privacy breach?

- o Yes (1)
- o No (2)

Page Break

Privacy Concern 1: How concerned are you about your online privacy (on a scale of 1–5)?

- o 1 - Not Concerned at All (1)
- o 2 - Slightly Concerned (2)
- o 3 - Moderately Concerned (3)
- o 4 - Very Concerned (4)
- o 5 - Strongly Concerned (5)

Privacy Concern 2: How concerned are you that your personal information could be misused (on a scale of 1–5)?

- o 1 - Not Concerned at All (1)
- o 2 - Slightly Concerned (2)
- o 3 - Moderately Concerned (3)
- o 4 - Very Concerned (4)
- o 5 - Strongly Concerned (5)

Privacy Concern 3: How concerned are you that your personal information could be accessed by unknown parties (on a scale of 1–5)?

- o 1 - Not Concerned at All (1)
- o 2 - Slightly Concerned (2)
- o 3 - Moderately Concerned (3)
- o 4 - Very Concerned (4)
- o 5 - Strongly Concerned (5)

Privacy Risk 1: Have you heard of the term "digital privacy risks"?

- o Yes (1)
- o No (2)

Privacy Risk 2: If yes, what would you consider to be the biggest digital privacy risks to you? Else type N/A.

_____

Page Break

Privacy Tools 1: Do you currently use any privacy-preserving tools on your smartphone?

- o Yes (1)
- o No (2)

Privacy Tools 2: Please select any of the following tools you use on your phone.

- Encryption Apps (1)
- VPNs (2)
- Ad Blockers (3)
- Password Managers (4)
- Privacy Focused Browsers (5)
- Antivirus Software (6)
- Locked Folders (7)
- Other (8)

Display This Question:

If Please select any of the following tools you use on your phone. = Other

Privacy Tools 3: If you select "Other" option in the above question, please mention it here.

_____

Privacy Tools 4: What is your primary reason for using privacy-preserving tools?

_____

Security Features: How familiar are you with the security features on your phone?

- o I have checked all the settings on my phone to secure it the best I can (1)
- o I change the default settings as issues come to my attention (2)
- o I use the default options (3)

Device: Is your primary smartphone device Rooted (Android) or Jail Broken (iOS) ?

- o Yes (1)
- o No (2)
- o I don't know these terminologies (3)

End of Block: Privacy Tools Usage

APPENDIX E. SURVEY RESPONSES FOR DIGITAL PRIVACY RISK CONCERN

Privacy Risk 2:
If yes, what would you consider to be the biggest digital privacy risks to you? Else type N/A.
the starting point for identity theft can be publicly available information on social media.
Data breaches, phishing attacks
Data Breaches Unauthorized access to sensitive information stored by organizations can lead to data breaches. This may result in the exposure of personal details, such as names, addresses, and financial information.
Data Breaches: Large-scale breaches of databases containing personal information.
database server breaches
Reusing weak passwords
digital surveillance
complying with regulations, preserving freedom of expression
Collecting more information than is needed.
One of the most significant risks associated with data sharing and collection is the potential for data breaches.
Address, Credit card number
Weak passwords, lack of two-factor authentication, and insufficient security measures on websites and applications contribute to the vulnerability of personal information.
Large-scale data breaches expose sensitive information, such as personal details, login credentials, and financial data. Cybercriminals often target databases of organizations to steal and sell this information on the dark web.
Data breaches and personal data availability.
malware
Social engineering, malware and data breaches
Data Mining and Profiling: Companies often collect and analyze vast amounts of user data to create detailed profiles for targeted advertising, which can lead to invasion of privacy and manipulation of consumer behavior.
Online privacy is involved in everything from how technology evolves to how this evolution impacts your personal safety and security
Data mining leading to identity theft
data breaches are the result of out-of-date software, weak passwords, and targeted malware attacks. Unfortunately, they can cost an organization a damaged reputation and a great deal of money.
social engineering, weak security practices
misuse of data
Data Breaches, Tracking and Profiling, Government Surveillance
data breaches, social engineering
data protection issues and privacy loopholes
the starting point for identity theft can be publicly available information on social media

data protection issues and privacy loopholes
Data Breaches, Tracking and Profiling, Government Surveillance
Data breaches
Reusing weak passwords is one of the leading causes for the massive data breaches.
Phishing Attacks, Data Breaches and Unsecured Wi-Fi Networks
Phishing Attacks, Data Breaches and Unsecured Wi-Fi Networks
Data breaches fuel cyberattacks
Data breaches and personal data availability
In most cases, data breaches are the result of out-of-date software, weak passwords, and targeted malware attacks. Unfortunately, they can cost an organization a damaged reputation and a great deal of money.
Data breaches and personal data availability.
according to me social media apps are very biggest digittal privacy risk.
Data breaches and personal data availability.
Data breaches: When sensitive information is accessed without authorization. Data breaches can be caused by weak passwords, out-of-date software, and malware attacks. Data breaches can expose personal data and fuel cyberattacks.
Identity theft and cybercrime.
Failing to establish effective barriers can leave sensitive data vulnerable to unauthorized access, theft, and misuse. Whether due to outdated security measures or lack of advanced protection tools, such vulnerabilities can jeopardize both individuals' data privacy and an organization's reputation.
one the biggest threats to your privacy. Reusing weak passwords is one of the leading causes for the massive data breaches you see in the news. That is because it allows cyber criminals to break into multiple accounts at once and engage in identity theft or financial fraud - often both.
Yes, I'm familiar with the term "digital privacy risks." In my opinion, the biggest digital privacy risks to individuals include data breaches, where personal information can be exposed to malicious actors. Another significant risk is online tracking, where companies monitor and collect data on users' browsing habits without their consent. Phishing attacks are also a major concern, as they can trick individuals into revealing sensitive information such as login credentials or financial details. Additionally, identity theft poses a serious threat, where hackers can use stolen information to impersonate someone else or commit fraud. Lastly, the potential for surveillance, whether by governments or corporations, raises concerns about the erosion of privacy rights in the digital age.
Cybercriminals remain the biggest threat due to shady practices · Use lengthy, complex, and varied passwords
Some principal modern privacy issues include digital surveillance, data breaches, identity theft, and cybercrimes.
Health Records
Data breaches: Companies may experience data breaches: allowing cybercriminals to access personal and sensitive information.
When companies or organizations experience data breaches, sensitive personal information such as names, addresses, passwords, and financial details can be exposed. This can lead to identity theft, fraud, and other malicious activities.
our bank details

data mining, data breach, third-party data sharing.
In most cases, data breaches are the result of out-of-date software, weak passwords, and targeted malware attacks. Unfortunately, they can cost an organization a damaged reputation and a great deal of money.
Data breaches and personal data availability.
As more devices become connected to the internet, such as smart home appliances and wearable technology, there is an increased risk of privacy breaches due to vulnerabilities in these devices' security protocols. Hackers could potentially access sensitive data or even control these devices remotely.
theft of our personal and bank details.
Online privacy is involved in everything from how technology evolves to how this evolution impacts your personal safety and security.
Data breaches and personal data availability.
In most cases, data breaches are the result of out-of-date software, weak passwords, and targeted malware attacks
insecure personal information
Health Records
BANK BALANCE LOW
hacking
Data breaches and personal data availability.
potential or actual actions targeting informational resources that lead to unauthorized access to protected data.
One of the most significant risks associated with data sharing and collection is the potential for data breaches.
hacking
one the biggest threats to your privacy. Reusing weak passwords is one of the leading causes for the massive data breaches you see in the news
Data breaches and personal data availability.
data breaches are the result of out-of-date software, weak passwords, and targeted malware attacks. Unfortunately, they can cost an organization a damaged reputation and a great deal of money.
Cybercriminals remain the biggest threat due to shady practices · Use lengthy, complex, and varied passwords.
using like fake links
Our virtual privacy services are tailored to fit the budget and maturity of your business. CompliancePoint has helped hundreds of companies in a range of industries mitigate risk.
Digital threats refer to potential or actual actions targeting informational resources that lead to unauthorized access to protected data.
Cybercriminals remain the biggest threat due to shady practices · Use lengthy, complex, and varied passwords.
data mining, data breach, third-party data sharing, privacy setting loopholes, location settings, harassment and cyberbullying, fake information, and malware and viruses.
Virulent computer viruses that can destroy data, damage hardware, cripple systems and disrupt a business' operations.

Data breaches. Health insurance information being leaked or banking information. Breaches of that nature.
Reusing weak passwords is one of the leading causes for the massive data breaches you see in the news
data, privacy,engineering
In most cases, data breaches are the result of out-of-date software, weak passwords, and targeted malware attacks. Unfortunately, they can cost an organization a damaged reputation and a great deal of money.
Theft or manipulation of sensitive or private information, such as financial or health records.
some of the biggest risks are outside of your control , like if a social media site is hacked.
Virulent computer viruses that can destroy data, damage hardware, cripple systems and disrupt a business' operations.
hackers can steel the personal information and including the credit card information also
some of the biggest digital privacy risk is hacking social media accounts and personal information mishandling.
personal information mishandling , hacking social media accounts ,snooping and location tracking.
sharing our personal information to others without our permission.
In most cases, data breaches are the result of out-of-date software, weak passwords, and targeted malware attacks. Unfortunately, they can cost an organization a damaged reputation and a great deal of money.
malware
Personal Data
Unauthorized access to my sensitive personal information stored by organizations could expose the data like credit card numbers, passwords and Social Security number.
potential or actual actions targeting informational resources that lead to unauthorized access to protected data. Understanding digital privacy generally involves discussing and addressing online privacy threats that businesses and consumers face
Data breaches
Health Records
HEALTH RECORDS
tracking, hacking and trading
one the biggest threats to your privacy.
HEALTH RECORD
It's about selling our data to third party companies for their profit.
Understanding digital privacy generally involves discussing and addressing online privacy threats that businesses and consumers face.
personal beliefs, purchasing habits, and even your daily routine can be assembled.
Digital threads refer to potential or actual action targeting informational sources that lead to unauthorised access to protected data.
One of the most significant risks associated with data sharing and collection is the potential for data breaches. Hackers can infiltrate databases and steal personal information, including names, addresses, phone numbers, and even credit card numbers

the “top 3” privacy issues with most data breaches are “tracking, hacking and trading.” Let's take a closer look at each one and see how it impacts your privacy.
Theft or manipulation of sensitive or private information, such as financial or health records.

APPENDIX F. SURVEY RESPONSES FOR USAGE OF PRIVACY-PRESERVING TOOLS

Privacy Tools 4:
What is your primary reason for using privacy-preserving tools?
empowers individuals to maintain control over their personal information.
The protection of the personal information
empowers individuals to maintain control over their personal information.
protecting personal information, maintaining anonymity
The protection of the personal information
My primary reason for using privacy-preserving tools is to protect my personal information and data from unauthorized access, surveillance, and exploitation. I want to ensure that my online activities are kept private and secure, and that my sensitive information is not being misused or shared without my consent. Additionally, I value my right to privacy and believe that it is important to take proactive steps to safeguard it in an increasingly digital world.
Privacy-preserving tools help individuals keep their personal information, such as names, addresses, financial details, and communication, secure from unauthorized access or exploitation.
Protecting Personal Information
For security
RISKS
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent
personal information
protecting personal data
empowers individuals to maintain control over their personal information
Data privacy empowers individuals to maintain control over their personal information. I
Data privacy empowers individuals to maintain control over their personal information
empowers individuals to maintain control over their personal information
he protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.
Data privacy empowers individuals to maintain control over their personal information.
empowers individuals to maintain control over their personal information
Privacy preserving tools will be useful to prevent from harmful virus and secure our personal details.
Protecting Personal Information
Individuals affected by a data breach may find improper financial and credit activity in their name, compromised social media accounts and other issues.
Privacy-preserving tools help prevent unauthorized access to sensitive data. By encrypting information and implementing secure access controls, these tools ensure that only authorized individuals can view or manipulate the data.

empowers individuals to maintain control over their personal information.
Protecting privacy is key to ensuring human dignity, safety and self-determination.
data security
protecting personal information
empowers individuals to maintain control over their personal information
safety precations
Data privacy empowers individuals to maintain control oveR
to safeguard a user's privacy by eliminating all traces of their activities.
empowers individuals to maintain control over their personal information.
Privacy-preserving tools help individuals safeguard their sensitive personal information, such as financial data, health records, and communication logs, from unauthorized access and exploitation.
for security
Healthcare: In the healthcare sector, PP ML plays a pivotal role in ensuring patient privacy.Oct
empowers individuals to maintain control over their personal information
It allows them to decide how their data is collected, used, and shared.
The primary reason for using privacy-preserving tools is to protect and safeguard individuals' personal information and sensitive data from unauthorized access, misuse, or exposure. Privacy-preserving tools are designed to ensure confidentiality, integrity, and security of user data, reducing the risk of privacy breaches and unauthorized disclosures. These tools employ encryption, anonymization, and other techniques to enable individuals to control and limit access to their personal information, fostering trust and providing a layer of defense against potential privacy threats in the digital age.
Empowers individuals to maintain control over their personal information.
Data privacy empowers individuals to maintain control over their personal information.
empowers individuals to maintain control over their personal information
Empowers individuals to maintain control over their personal information.
Empowers individuals to maintain control over their personal information.
empowers individuals to maintain control over their personal information.
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service .
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
I HAVE MULTI DOCUMENTS IN THIS DEVICE.
protecting personal informations
protecting personal information
DATA SECURITY
SAFETY & SECURE THE PHONE
Protecting Personal Information: To safeguard sensitive data such as financial information, health records, or personal communications from unauthorized access or misuse.
protecting personal informations
SAFETY & SECURE THE PHONE

DATA SECURITY
Very sequence
Avoid getting scammed, phished etc
empowers individuals to maintain control over their personal information.
empowers individuals to maintain control over their personal information
To save my data and protect it
For privacy and security.
secure the data
smartphones
Government SurveillanceProtecting Personal Information: To safeguard sensitive data such as financial information, health records, or personal communications from unauthorized access or misuse.
SOME PEOPLE MISUSE OUR MEDIA FILES THROUGH SOCIAL MEDIA. SO I PROTECT THAT BY USING THESE TOOLS.
Maintain anonymity
NOT LIKE TO SHARE.
Protecting Personal Information, Preventing Identity Theft and Maintaining Confidentiality
Protecting Personal Information, Preventing Identity Theft and Maintaining Confidentiality
Data De-identification
empowers individuals to maintain control over their personal information.
Empowers individuals
FOR PRPIVATE CHATS DOWNLOADS
As a language model AI developed by OpenAI, I do not have personal reasons for using privacy-preserving tools. However, individuals typically use privacy-preserving tools to protect their personal data, maintain their online anonymity, prevent tracking by advertisers, and safeguard their privacy from surveillance by governments and other entities.
empowers individuals to maintain control over their personal information.
To protect my data
Data privacy empowers individuals to maintain control over their personal information.
empowers individuals to maintain control over their personal information.
Data privacy empowers individuals to maintain control over their personal information
EMPOWERS INDIVIDUALS TO MAINTAIN CONTROL OVER THEIR PERSONAL INFORMATION
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
Data privacy empowers individuals to maintain control over their personal information.
for personal safety and data privacy
sensor
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
SECURITY
secure finance transaction

protect the privacy of their personally identifiable information (PII) provided to and handled by service
internet
My primary reason for using privacy-preserving tools is to protect my personal information and data from being accessed or misused by unauthorized individuals or organizations. I also want to maintain my online anonymity and ensure that my online activities are not monitored or tracked without my consent. Additionally, I value my privacy and believe that it is important to take steps to safeguard it in today's digital age.
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
SECURITY AND SAFETY
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
There's a growing awareness of the ethical implications of data collection and surveillance. Many people choose privacy-preserving tools to support ethical practices and promote a more transparent and equitable digital environment.
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
My primary reason for using privacy-preserving tools is to protect my personal information and keep it safe from unauthorized access or misuse. I value my privacy and want to ensure that my data is not being exploited or shared without my consent. Using these tools helps me feel more secure and in control of my online presence.
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
Data privacy empowers individuals to maintain control over their personal information.
empowers individuals to maintain control over their personal information.
Privacy preserving technologies (PPTs) offer comprehensive data protection capabilities that minimize personal data use and maximize data security, while enabling marketers to gain campaign insights, analyze audience data and optimize their reach.
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
My primary reason for using privacy-preserving tools is to protect my personal information and maintain control over how it is shared and used online. I value my privacy and want to minimize the risk of my data being misused or exploited by companies or malicious actors. By using these tools, I can feel more secure in my online activities and be confident that my information is protected.
cyberthreats
Because it empowers me to maintain control over my personal information. It allows me to decide how the data is collected, used, and shared. Data privacy ensures that my personal information is not exploited or misused without consent.
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
Data privacy empowers individuals to maintain control over their personal information
Data privacy empowers individuals to maintain control over their personal information. I
PROTECT SENSITIVE INFORMATION
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.

Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
empowers individuals to maintain control over their personal information
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
Data privacy empowers individuals to maintain control over their personal information.
My primary reason for using privacy-preserving tools on my smartphone is to protect my personal information and online activities from unauthorized access, surveillance, and exploitation. I value my privacy and want to minimize the risk of data breaches, identity theft, and invasive tracking by companies and malicious actors.
Ensure that there could be no potential problems on my phone, such as viruses and malware.
The Open Data movement is excellent for data about bacteria, plants or animals, but we need to be more careful with human data.
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
Data privacy empowers individuals to maintain control over their personal information.
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
Data privacy empowers individuals to maintain control over their personal information.
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
Data privacy empowers individuals to maintain control over their personal information.
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
To product my data
Secure Server
The primary reason for using privacy-preserving tools is to protect personal information and ensure online privacy
empowers individuals to maintain control over their personal information.
empowers individuals to maintain control over their personal information.
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared.
My primary reason for using privacy-preserving tools is to protect my personal information and ensure that my online activities are not tracked or monitored by third parties. I value my privacy and want to have control over who has access to my data. Using these tools helps me feel more secure and confident in my online interactions.
Preventing Surveillance: Individuals concerned about government or corporate surveillance may use privacy-preserving tools to encrypt their communications, mask their IP addresses, and minimize the collection of metadata.

privacy preserving technologies allow users to protect the privacy of their personally identifiable information PII provided to and handled by service providers or apps all while allowing marketers to maintain the functionally of data driven systems.
rivacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
I use it to keep my personal photos, videos and information from leaking from my phone.
Data privacy empowers individuals to maintain control over their personal information. I
protect a privacy by removing all traces of their activity.
for my personal safety.
empowers individuals to maintain control over their personal information
Data privacy empowers individuals to maintain control over their personal information.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
Privacy preserving tools used for safety and security for secret information
Data privacy empowers individuals to maintain control over their personal information.
SAFTY
smart phone
Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent

My primary reason for using privacy-preserving tools is to protect my personal information from being accessed or shared without my consent. I value my privacy and want to ensure that my online activities and communications remain private and secure. Additionally, using privacy-preserving tools helps me feel more in control of my data and reduce the risk of identity theft or other malicious activities.
SMART PHONE
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service ...
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
To secure and protect my personal information.
MY SAFETY AND MY PERSONAL INFORMATION ARE VERY IMPORANT
The primary reason for using privacy-preserving tools is to protect sensitive information and maintain confidentiality. These tools help individuals and organizations safeguard their personal data and prevent unauthorized access, misuse, or disclosure of information. By using privacy-preserving tools, individuals can ensure their online activities, communications, and transactions remain secure and private, reducing the risk of identity theft, surveillance, and other privacy violations.
SAFTEY
Data privacy empowers individuals to maintain control over their personal information.
Privacy-preserving tools can help protect individuals' right to free speech by enabling them to communicate and express their opinions without fear of censorship or reprisal.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information.
Most of the security and privacy issues occur due to improper data processing. Not only that, but most cases are caused by in-house data processing. And yet, many organizations and individuals still believe they don’t have anything to worry about since they only work with data internally. This is obviously a myth.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
for my personal safety.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
Preserving Individual Autonomy: Data privacy empowers individuals to maintain control over their personal information. It allows them to decide how their data is collected, used, and shared. By respecting individuals' autonomy, data privacy ensures that personal information is not exploited or misused without consent.
These tools aim to prevent unauthorized access, tracking, or misuse of personal data by individuals, corporations, or governments

SOME WEBSITE ACCESS TIME EASY WAY TO HACK, SO I USE PRIVACY PRESENTING TOOLS
Data privacy empowers individuals to maintain control over their personal information.
PERSONAL SAFE
empowers individuals to maintain control over their personal information
Data security
empowers individuals to maintain control over their personal information
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
to make sure that my personal information is not leaked
Preserving privacy
For Safety
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
malware attack
HIDE PASSWORDS
MAINTAINING TRUST AND CONFIDENCE
It is very easy
safety purpose
To avoid ads
The Open Data movement is excellent for data about bacteria, plants or animals
MAINTAINING TRUST AND CONFIDENCE
safety
MY THOUGHT
By preserving privacy, individuals can have control over who has access to their personal information,
Privacy preservation plays a vital role in maintaining trust and confidence between individuals and organizations.
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service .
safety
differential privacy (DP), and tunnel encryption
Personal data secure
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
Privacy-preserving machine learning offers innovative solutions across diverse industries by harnessing the power of data
Privacy-preserving machine learning offers innovative solutions across diverse industries by harnessing the power of data while safeguarding sensitive information. For example, it can be used in: Healthcare: In the healthcare sector, PPML plays a pivotal role in ensuring patient privacy.
safety
Maintaining Trust and Confidence

preserving privacy, individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse. 2. Maintaining Trust and Confidence
Privacy-preserving machine learning offers innovative solutions across diverse industries by harnessing the power of data while safeguarding sensitive information.
FOR PRIVACY SAFETY.
i need some privacy tools thats why am using
preserving privacy, individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse. 2. Maintaining Trust and Confidence
Data privacy is important for several key reasons: Protection of Personal Information
rivacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
Privacy preservation processing techniques intend to blur or even break the link between sensitive data and the originate owner (i.e. the source) without critically affecting its capability to provide valuable insights about a certain phenomenon of interest (i.e. ensuring privacy while minimizing information loss).
FOR PRIVACY SAFETY.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse. 2. Maintaining Trust and Confidence: Privacy preservation plays a vital role in maintaining trust and confidence between individuals and organizations
Privacy-preserving machine learning offers innovative solutions across diverse industries by harnessing the power of data while safeguarding sensitive information. For example, it can be used in: Healthcare: In the healthcare sector, PPML plays a pivotal role in ensuring patient privacy.
purpose of these tools, be they open-source, free, or commercial, is to protect a user's privacy by removing all traces of their activity.
MAINTAINING TRUST AND CONFIDENCE
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
its using to protecting my data.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
I don't like being tracked.
FOR AN SECURITY PURPOSE
MAINTAINING TRUST AND CONFIDENCE
it can be used in: Healthcare: In the healthcare sector, PPML plays a pivotal role in ensuring
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
To protect a user's privacy by removing all traces of their activity

The marketed purpose of these tools, be they open-source, free, or commercial, is to protect a user's privacy by removing all traces of their activity.
to protect my device from virus and hacking
personal work
very usefull
protection of personal information.
The marketed purpose of these tools, be they open-source, free, or commercial, is to protect a user's privacy by removing all traces of their activity.
process of removing the limitations on a mobile or tablet running the Android operating system.
for my personal information
SAFETY
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
protection of personal information.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
protecting privacy is key to ensuring human dignity, safety and self - determination.
protection of personal information.
for my own safety
ndividuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
ensuring privacy while minimizing information loss
control over who has access to their personal information, mitigating the risk of identity theft
Privacy-preserving machine learning offers innovative solutions across diverse industries by harnessing the power of data while safeguarding sensitive information. For example, it can be used in: Healthcare: In the healthcare sector, PPML plays a pivotal role in ensuring patient privacy.
protect the privacy of personal information
to protect personal information
SAFE
data security
Password secure
SAFE
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
I use ad blockers primarily to enhance my online privacy and security by blocking intrusive advertisements and preventing tracking by advertisers.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
Human right to privacy

Human right to privacy
It relates to an individual's ability to determine for themselves when, how, and for what purpose their personal information is handled by others. Protecting privacy is key to ensuring human dignity, safety and self-determination. It allows individuals freely develop their own personality.
Secure Browser
processing techniques intend to blur or even break the link between sensitive data and the originate owner
FOR SECURITY
my privacy preserving tools aredifferential privacy (DP), and tunnel encryption (e.g. SSL) and Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
protect the privacy of their personally identifiable information provided to and handled by service
I Got some spam/theft messages so i use privacy preserving tool
Privacy preservation processing techniques intend to blur or even break the link between sensitive data and the originate
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
The marketed purpose of these tools, be they open-source, free, or commercial, is to protect a user's privacy by removing all traces of their activity and differential privacy (DP), and tunnel encryption (e.g. SSL)
the protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
Privacy-preserving machine learning offers innovative solutions across diverse industries by harnessing the power of data while safeguarding sensitive information. For example, it can be used in: Healthcare: In the healthcare sector, PPML plays a pivotal role in ensuring patient privacy
differential privacy (DP), and tunnel encryption .
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
Protecting privacy is key to ensuring human dignity, safety and self-determination.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
SECURITY
SAFETY OF THE DATA
Maintaining Trust and Confidence: Privacy preservation plays a vital role in maintaining trust and confidence between individuals and organizations.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.

individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud
personal information
DATA SHARING IS THE ENEMY OF PRIVACY PRESERVATION
personal information
DATA SAFETY
To secure my data
personal information
personal information
theif
to secure my data
DATA SECURITY
personal information
Protecting privacy is key to ensuring human dignity, safety and self-determination.
personal information
theif
personal information
Protecting sensitive personal information from being accessed by unauthorized parties. Preventing online tracking and targeted advertising. Safeguarding against identity theft and fraud. Maintaining anonymity while browsing the internet. Ensuring confidentiality in communication and data sharing. Exercising control over personal data and digital privacy. Complying with privacy regulations and guidelines.
personal information
TO ACHIEVE PRIVACY PROTECTION BY DIFFERENT DATA CHARACTERISTICS IN HIGH LEVEL DATA
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
TO ACHIEVE PRIVACY PROTECTION BY DIFFERENT DATA CHARACTERISTICS IN HIGH LEVEL DATA
By preserving privacy, individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
https://www.google.com/search?q=What+is+your+primary+reason+for+using+privacy-preserving+tools%3F&sourceid=chrome&ie=UTF-8#:~:text=By%20preserving%20privacy%2C%20individuals%20can%20have%20control%20over%20who%20has%20access%20to%20their%20personal%20information%2C%20mitigating%20the%20risk%20of%20identity%20theft%2C%20fraud%2C%20or%20misuse.
SECURE MY PERSONAL DATA AND IMPORTANT DOCUMENT OF MINE.
TO ACHIEVE PRIVACY PROTECTION BY DIFFERENT DATA CHARACTERISTICS IN HIGH LEVEL DATA
TO ACHIEVE PRIVACY PROTECTION BY DIFFERENT DATA CHARACTERISTICS IN HIGH LEVEL DATA
By preserving privacy, individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
Protecting privacy is key to ensuring human dignity, safety and self-determination.
safeguard sensitive information from unauthorized access

individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse
individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
MAINTAINING TRUST AND CONFIDENCE
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
It relates to an individual's ability to determine for themselves when, how, and for what purpose their personal information is handled by others. Protecting privacy is key to ensuring human dignity
Privacy preserving technologies allow users to protect the privacy of their personally identifiable information (PII) provided to and handled by service
TO ACHIEVE PRIVACY PROTECTION BY DIFFERENT DATA CHARACTERISTICS IN HIGH LEVEL DATA
Protecting privacy is key to ensuring human dignity, safety and self-determination. It allows individuals freely develop their own personality.
maintaining confidence and trust
Protecting datas and softwares
By preserving privacy, individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse.
Privacy preservation processing techniques intend to blur or even break the link between sensitive data and the originate owner (i.e. the source) without critically affecting its capability to provide valuable insights about a certain phenomenon of interest (i.e. ensuring privacy while minimizing information loss).
Maintaining Trust and Confidence: Privacy preservation plays a vital role in maintaining trust and confidence between individuals and organizations.
By preserving privacy, individuals can have control over who has access to their personal information, mitigating the risk of identity theft, fraud, or misuse. 2. Maintaining Trust and Confidence: Privacy preservation plays a vital role in maintaining trust and confidence between individuals and organizations