International Review of Social Sciences Research
Volume 4 Issue 4 December 2024
DOI: https://doi.org/10.53378/irssr.353125

Filipino attitude and perception on Subscriber Identity Module (SIM) Card Registration Act

[1]Aera L. Diaz & [2]Romano M. Balbacal

Abstract

The SIM Card Registration Act, a legislative initiative in the Philippines, mandates the registration of Subscriber Identity Module (SIM) cards to enhance security, monitor mobile phone usage, and curb crimes such as fraud, terrorism, and phishing. This phenomenological study explores the attitude and perceptions of individuals on the implementation of the Act, with a focus on how it impacts their sense of security, privacy, and everyday mobile phone use. Semi-structured interviews were conducted with 15 participants, aged 16 to 64, from the different barangays in San Pablo City, Laguna, Philippines. Data were analysed thematically, capturing participants' unique perspectives on the benefits and risks associated with the Act. The findings reveal that while participants acknowledged the Act's potential to prevent crimes and phishing, concerns about personal data security and the possibility of identity theft were prevalent. Participants' attitudes toward the Act were shaped by their experiences with mobile phone technology and privacy concerns, with older respondents expressing heightened sensitivity to data privacy. These insights underscore the need for more robust security measures in the registration process to enhance public trust. The study concludes with recommendations to improve user experience and safeguard personal information, offering a foundation for policy refinements and further research.

Keywords: *crime prevention, identity theft, sim card registration act, phishing incidents*

Article History:

***Received**: September 18, 2024*
***Revised**: October 29, 2024*
***Accepted**: October 31, 2024*
***Published online**: November 19, 2024*

Suggested Citation:
Diaz, A.L. & Balbacal, R.M. (2024). Filipino attitude and perception on Subscriber Identity Module (SIM) Card Registration Act. *International Review of Social Sciences Research*, 4(4), 58-79. https://doi.org/10.53378/irssr.353125

About the authors:
[1]Corresponding author. Master in Public Administration, Job Order, City Information Office San Pablo City Local Government Unit. Email: aeradiaz@gmail.com

[2]Doctor of Public Administration. Faculty in National University, Department of Education, and Pamantasan ng Lungsod ng San Pablo.

1. Introduction

The rapid evolution of communication technologies has significantly altered how people connect and interact. Platforms such as Facebook, Twitter, Instagram, Viber, WhatsApp, and SMS have become integral to daily life, reshaping social interactions and information sharing (Lee et al., 2020). These digital platforms, coupled with mobile applications like online banking and loan lending apps, have streamlined daily tasks, enhancing accessibility and convenience (Galván, 2019). However, this technological advancement also brings concerns about the overuse of information and communication technology (ICT), potentially undermining genuine human connections (Lee et al., 2020). Consequently, there is an emerging need for a balanced approach to digital engagement to preserve the essence of interpersonal relationships (Kim, 2019).

Among these technological innovations, the cell phone stands out as a pivotal advancement, revolutionizing communication by offering a swift and convenient means of connection in an increasingly fast-paced world (Lu, 2020). The reliance on cell phones extends beyond communication, as they have become essential tools for productivity, entertainment, and navigation (Ahmad, 2020). This reliance underscores the profound impact of cell phones on modern society's communication dynamics (Miller et al., 2019). At the heart of this functionality lies the Subscriber Identity Module (SIM) card, a small yet crucial component that stores mobile subscriber information, enabling phone connection to mobile networks for calling, texting, and data access (Airalo, 2022).

Despite the benefits, SIM cards have also been exploited for criminal activities, raising significant cybersecurity concerns. According to the 2023 report by the National Cyber Security Index (NCSI), countries like Greece, Lithuania, Belgium, Estonia, and the Czech Republic rank highest in terms of cybercrime victimization. In the Asia-Pacific region, China reported a staggering 14,157,775 data breach cases, followed by Japan and South Korea with 1,246,373 and 1,699,124 cases, respectively, in the third quarter of 2022. Phishing, often a precursor to more severe cybercrimes like ransomware, has been particularly problematic, as hackers exploit personal details such as email addresses, contact numbers, and bank account information (NCSI, 2023).

In the Philippines, the situation is equally alarming. The Philippine National Police Anti-Cybercrime Group (ACG) reported 4,254 SIM card-related offenses from January to September 2022, including online scams, bank fraud, and text scam activities (Cabalza, 2022).

The rise in such crimes underscores the vulnerability of mobile communication systems to exploitation. To address this growing threat, the Philippine government enacted Republic Act No. 11934, also known as the SIM Card Registration Act, on October 10, 2022. This law mandates the registration of all SIM cards, aiming to curb cybercrimes by equipping law enforcement agencies with the necessary tools to trace and address crimes involving SIM cards.

The introduction of mandatory SIM card registration in the Philippines mirrors global efforts to combat fraud and crime through similar policies. As of 2021, 157 countries had implemented SIM card registration policies, primarily targeting the reduction of cybercrime (GSMA, 2021). However, the Philippine experience has been challenging. Despite the government's efforts, by July 25, 2023, only 105 million of the 168.9 million active SIM cards had been registered, leading to concerns about the effectiveness of the registration campaign (Chi, 2023). The deactivation of unregistered SIM cards poses risks to users, including the loss of essential mobile services, which could hinder emergency communication, social interactions, and access to critical services like mobile banking (Luna, 2023).

The urgency of addressing SIM card-related crimes is highlighted by the surge in complaints received by the Philippine National Police – Anti-Cybercrime Group (PNP-ACG). In Region IV-A alone, the PNP-ACG reported a sharp increase in fraudulent activities linked to SIM card usage, with mobile banking applications like GCash emerging as significant sources of scams. This trend underscores the need for enhanced public awareness and stronger cybersecurity measures to mitigate the risks posed by online fraud. Despite the enactment of the SIM Card Registration Act, there remains a significant gap in understanding how it is experienced and perceived at the local level. This lack of clarity is not just a logistical issue but highlights the deeper challenge of effectively balancing regulation with public awareness and compliance, particularly as users' behaviors and perceptions play a critical role in the law's impact on cybersecurity (Blancaflor et al., 2023). In the digital era, where smartphones and contact numbers have become integral to daily life, exposure to cybersecurity threats such as smishing attacks has increased. Smishing, a social engineering attack using text messages to deceive recipients into revealing sensitive information or downloading malware, continues to exploit registered numbers, underscoring the need for robust cybersecurity measures.

This study seeks to explore the lived experiences of residents in San Pablo City, Laguna, Philippines focusing on their perceptions of the Act's implementation. Through an in-

depth examination of participants' insights, this study aims to understand their awareness, compliance, and views on the Act's impact on cybersecurity and crime prevention, while also identifying opportunities for improving registration procedures and addressing public concerns.

2. Literature review

2.1. Impact and Implementation of SIM Card Registration Laws

The integration of mobile phones into daily life has dramatically transformed communication and personal management. Modern mobile phones support a variety of activities, from gaming and online streaming to financial transactions and navigation, facilitated by their advanced features like GPS and built-in cameras (Kanishka, 2023). Their portability and efficiency make them essential tools for managing schedules, conducting remote work, and continuous learning. These functions underscore the critical role of mobile phones in contemporary society, reinforcing their status as indispensable devices that enhance convenience and connectivity.

Central to the operation of mobile phones is the SIM card, which serves as a crucial authentication and storage device. SIM cards enable network access, verify subscriber identities, and protect user data (Zhen et al., 2019). They were originally designed to facilitate mobile network connectivity and accurate billing for airtime usage, while also storing essential information such as phone directories and messages (La Torre et al., 2020). This multifunctionality highlights the SIM card's pivotal role in ensuring both connectivity and security in mobile communications. Despite their essential functions, traditional SIM cards present several challenges. These include issues related to size variations, complexity in switching carriers, and susceptibility to malfunctions (Airalo, 2022). Additionally, the process of replacing or managing multiple SIM cards can be cumbersome, especially during travel. These limitations underscore the need for more efficient and user-friendly solutions in mobile connectivity.

A SIM card functions as a secure microcontroller, storing unique identification data for each mobile subscriber and enabling communication within cellular networks (Khalili, 2022). SIM cards primarily authenticate users with the network, store contact information, and facilitate encrypted communication, thus safeguarding user data. However, the standardized nature of SIM technology also renders it susceptible to criminal activities. For instance,

attackers can exploit SIM cards via social engineering, SIM swapping, and smishing, manipulating the card's authentication role to access sensitive data or impersonate users (Blancaflor et al., 2023). These technical vulnerabilities highlight the importance of integrating robust security practices in SIM management to mitigate the risk of exploitation, especially as cybercrime tactics continue to evolve.

The misuse of SIM cards for criminal activities, such as phishing and fraud, has become a significant concern. The rise of SIM swap fraud, where criminals gain unauthorized control over a phone number, highlights the vulnerabilities associated with SIM card security (Bowyer & Bowyer, 2023). Smishing, a form of phishing conducted via SMS, further exacerbates this issue by tricking individuals into divulging personal information through deceptive links (Marks, 2021). These threats emphasize the need for robust measures to protect users from emerging cyber threats. In response to these challenges, the Philippine government enacted the SIM Card Registration Act to address issues related to text message crimes and enhance mobile security. The Act mandates the registration of all SIM cards, including those used by foreign nationals, to ensure proper identification and reduce fraudulent activities (Republic Act No. 11934, 2022). This legislation includes provisions for confidentiality and penalties for non-compliance, reflecting the government's commitment to improving security and privacy in mobile communications.

Governments worldwide have implemented regulatory frameworks to manage and reduce criminal activities associated with SIM card use. Policies such as mandatory SIM card registration require users to verify their identity before activation, making it more difficult for criminals to remain anonymous and engage in fraudulent schemes (Wanja, 2021). Furthermore, regulatory agencies work alongside telecommunications providers to establish real-time monitoring systems that can detect suspicious patterns, such as repeated SIM replacements or high-volume registrations, which may indicate criminal intent (Gundur et al., 2023). Beyond regulation, government-led public awareness campaigns aim to educate citizens on safeguarding personal information from scams such as smishing and SIM swapping, which exploit SIM technology for unauthorized access to user accounts and financial data (Kim et al., 2022). These combined efforts reflect a proactive governmental role in protecting users and adapting to the security challenges posed by rapidly advancing digital communication technologies.

Section 4 of the SIM Card Registration Act outlines comprehensive regulations for SIM registration, mandating that all SIM cards be registered before activation. The law requires all end-users, including those with embedded SIMs and data-only SIMs, to complete the registration process. Failure to comply results in the non-activation of SIMs, with additional provisions for temporary validity for foreign nationals. This regulatory framework aims to enhance compliance and security across various user groups. The implementation of the SIM Card Registration Act involves collaboration among government agencies and service providers to facilitate registration, especially in remote areas. The Act mandates that registration be conducted at no cost to end-users, ensuring accessibility. This collaborative approach is intended to streamline the registration process and increase its effectiveness in combating mobile-related crimes.

Globally, the adoption of SIM card registration laws has varied, with 157 countries implementing such policies since their inception (Privacy International, 2019). However, these laws have faced challenges, including concerns about data security and effectiveness in crime prevention. For instance, Mexico's experience with SIM card registration highlighted issues related to implementation and efficacy, while Pakistan's case demonstrated the emergence of a black market and increased identity theft (Privacy International, 2019).

In the context of the Philippines, the SIM Card Registration Act reflects a broader global trend towards enhancing mobile security. However, the effectiveness of such legislation depends on its implementation and the broader regulatory environment. As noted by Manticajon (2023), while SIM card registration can contribute to reducing online scams and disinformation, it should be complemented by comprehensive digital literacy programs and robust regulations from social media platforms to address the complexities of the digital landscape effectively.

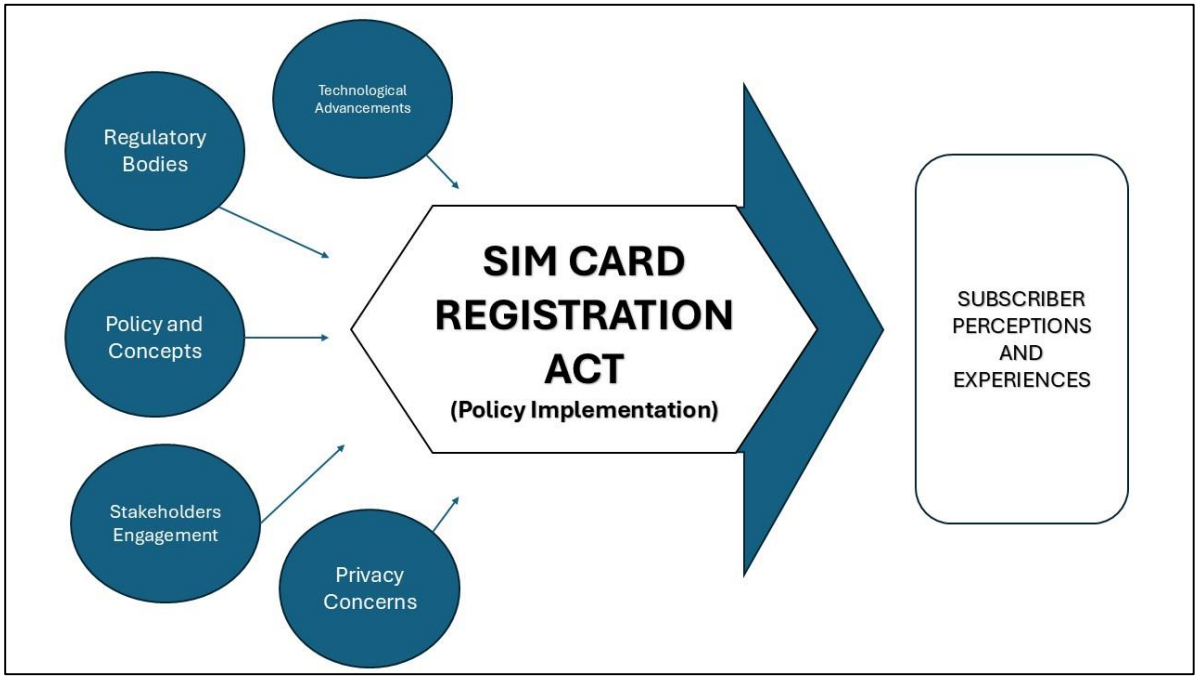
Studies on SIM card registration practices reveal variations in demographic impacts and user perceptions. For example, Stark (2021) found that in Dar-es-Salaam, Tanzania, mobile phone users fell within the 29 to 39 age range, with all age groups potentially owning SIM cards. In the Philippines, minors can purchase SIM cards with registration conducted under the name of their guardians. Gender dynamics also play a role, with studies indicating differences in registration practices and privacy concerns between men and women (Ahmed et al., 2019).

The implementation of biometric registration for SIM cards in 24 countries underscores a growing trend towards enhancing security measures (Bischoff, 2023). This approach aims to address challenges related to SIM card misuse and identity theft, highlighting the need for continuous adaptation of registration practices to meet evolving security demands. Overall, the literature emphasizes the importance of effective SIM card registration in improving mobile security while acknowledging the need for comprehensive strategies to address the broader challenges of the digital age.

2.2. Theoretical Framework

Figure 1

Graphical representation of the framework of the study



This study employs the Public Policy Implementation Theory developed by Leonid Hurwicz (1979) to analyze the practical application of the SIM Card Registration Act (RA 11934). Hurwicz's theory emphasizes the challenges and strategies involved in transforming policy concepts into effective real-world outcomes. It addresses how to establish institutions and processes that can successfully translate theoretical policies into tangible results, particularly amidst complex real-world conditions and divergent stakeholder interests (Howlett, 2018). The framework provides a structured approach to examining the evolution of

the SIM Card Registration Act from its initial formulation to its current implementation, highlighting the theory's role in identifying critical issues, setting clear objectives, and devising effective strategies.

The theory's application extends to stakeholder engagement, underscoring the need for their active involvement and alignment with policy goals to ensure successful implementation (Salem, 2021). Regulatory bodies and mobile operators, as key players, adhere to the theory's principles by facilitating compliance, coordinating efforts, and addressing emerging challenges (Birkland, 2019). Additionally, the theory informs technological advancements designed to support the policy's objectives while protecting data security (Mugambwa et al., 2020). It also guides the registration process by addressing compliance, privacy concerns, and communication effectiveness. Through a focus on compliance monitoring and enforcement, the theory ensures that the policy is applied fairly and effectively, optimizing its overall impact (Sabatier, 2019). Ultimately, Hurwicz's Public Policy Implementation Theory offers a comprehensive framework for understanding and enhancing the implementation of the SIM Card Registration Act.

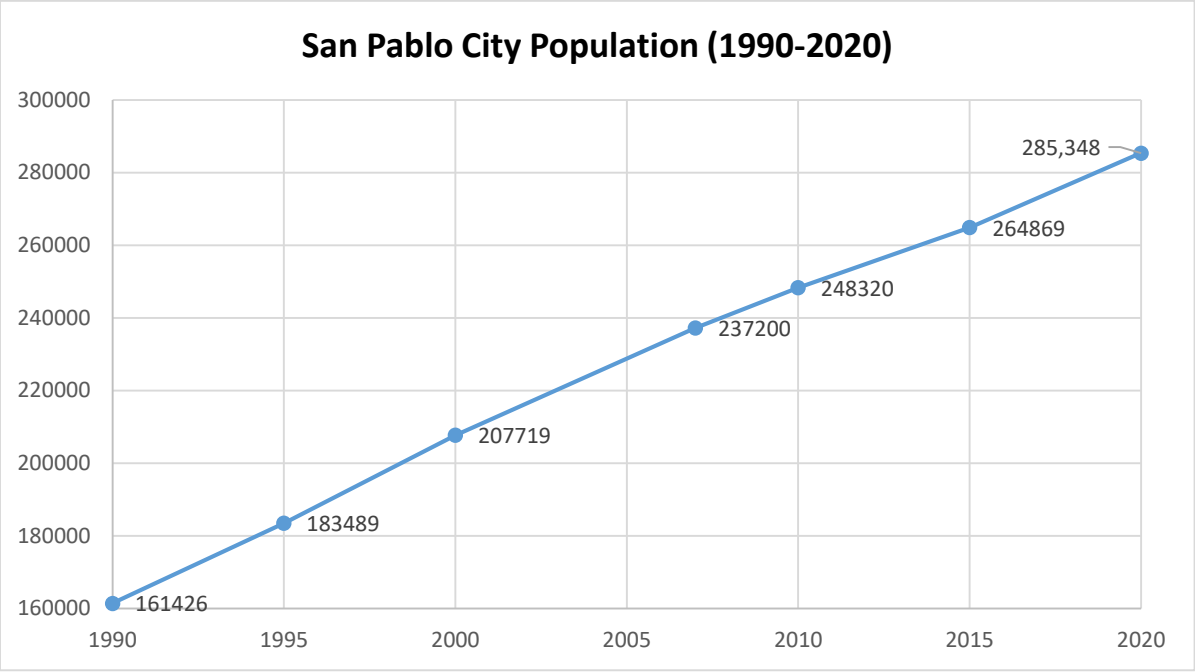
3. Methodology

This study employs a qualitative phenomenological research design to explore the lived experiences and perceptions of residents in San Pablo City, Laguna, regarding the SIM Card Registration Act. Phenomenology, as a research approach, aims to uncover and describe how individuals experience a particular phenomenon in their everyday lives. This design is appropriate for the study as it seeks to provide a deep understanding of participants' perceptions, attitudes, and concerns related to the Act's implementation, as well as its impact on their sense of security, privacy, and compliance with the law.

The study was conducted in San Pablo City, Laguna, one of the largest cities in the province. The three most populous barangays were selected as the research sites, representing diverse social, economic, and demographic backgrounds. The barangays were chosen to ensure a wide range of perspectives on how the Act affects different segments of the population. These communities were particularly relevant as they are urbanized areas where mobile phone usage is high, and the population is more likely to be engaged with SIM card registration procedures.

Figure 1

San Pablo City Population from 1990 to 2020



***Source**:* Philatlas.com

Participants were selected through purposive sampling, a non-probability sampling technique often used in qualitative research. A total of 15 participants aged between 16 and 60 were recruited for the study, representing a diverse range of socio-demographic profiles including gender, age, occupation, and mobile phone usage habits. The sample size was determined based on the principle of data saturation, whereby additional interviews no longer yielded new insights or themes. Participants were recruited through local community leaders, social networks, and online platforms. The inclusion criteria required participants to be residents of San Pablo City and to have completed the SIM card registration process. Data were collected using semi-structured interviews, which allowed for in-depth exploration of participants' perceptions while providing flexibility to probe for additional insights as the conversations unfolded. An interview guide was developed to cover key areas such as participants' understanding of the SIM Card Registration Act, their registration experiences, perceived benefits and risks, concerns about data security and privacy, and views on the Act's overall effectiveness in crime prevention. The guide was designed to elicit rich, detailed responses while ensuring that all key aspects of the research questions were addressed. Interviews were conducted in Filipino. All interviews were audio-recorded with the

participants' consent and subsequently transcribed verbatim. Transcription was completed manually to ensure accuracy and capture the full content of each conversation for analysis. Field notes were also taken during the interviews to capture non-verbal cues and other contextual information that could enrich the analysis. Data were analyzed using thematic analysis, following the six-step framework proposed by Maguire and Delahunt (2017 as cited by Gonzales & Villacruel, 2024).

Maguire and Delahunt's six-step framework for thematic analysis provides a structured approach to analyzing qualitative data. The process begins with familiarization, which involves reading through the data multiple times to capture its depth and overall meaning, while noting significant points. Next, initial codes are generated, assigning specific labels to relevant phrases or sections that capture essential ideas connected to the research questions. In the third step, connections among the codes are identified to group them into broader themes representing key topics within the data. Reviewing themes is the fourth step, where these initial themes are refined to ensure they accurately represent the data, eliminating overlap or adjusting divisions as needed. The fifth step involves defining and naming the themes to clarify what each theme represents and how it contributes to understanding the data. The final step is writing up the report, presenting themes with illustrative quotes from the data to convey insights gained through the analysis. This framework ensures a thorough and systematic examination of qualitative data.

The study adhered to the ethical principles outlined in the Data Privacy Act of 2012 (RA 10173) to ensure the protection of participants' rights and confidentiality throughout the research process. Key ethical considerations included informed consent, voluntary participation, confidentiality, and data security.

4. Findings and Discussion

The findings from this study offer valuable insights into the residents' lived experiences with the SIM Card Registration Act. The thematic analysis revealed a mixture of perceived benefits, concerns, and challenges that reflect broader societal and individual-level apprehensions about privacy, security, and governance.

Table 1 shows the summary of the themes, sub-themes and coded responses following the six-step framework for thematic analysis.

Table 1

Themes, sub-themes, and representative codes

Themes	Sub-Themes	Coded Response
Perceived Effectiveness in Crime Prevention	Prevention of phishing and fraud.	It helps prevent fraud.
	General public safety	I feel safer knowing criminals can be traced. It's a good law for public safety. Less anonymous numbers mean fewer crimes.
Data Security Concerns	Fear of identity theft	My information might be used for something else. Hackers might steal my data.
	Lack of trust in the government	I don't trust that the government will keep my data safe. What if my information is leaked?
Impact on Privacy	Loss of personal freedom	I feel like my every move is tracked.
	Overreach of government control	How far will they go to monitor us?
Registration Process Challenges	Inconvenience in the process	The process was confusing.
	Technical issues	It was hard to get the confirmation.
Differing Perceptions by Age	Younger individuals (16-30)	It's no big deal for me, everything is online. I'm used to sharing my data for apps.
	Older individuals (31-60)	Privacy is something we should protect more.

Note: Responses were all translated to English with the help of two intercoder

Perceived effectiveness in crime prevention. The perception of the SIM Card Registration Act as a preventive measure against cybercrime, particularly phishing and fraud, was a consistent theme among participants. Most respondents expressed a sense of increased safety, believing that the mandatory registration of SIM cards could reduce the anonymity often exploited by criminals. As one participant succinctly put it, "*I feel safer knowing criminals can be traced,*" reflecting a shared belief that the Act deters malicious activities by establishing a direct link between individuals and their mobile numbers. This perspective underscores the public's alignment with the government's rationale for enacting the law, which explicitly aims to curb cybercrime and reduce the use of unregistered SIM cards in criminal activities. This aligns with AlMarshoud et al., (2022) observation that increased accountability through registration can enhance user trust in mobile communications. The positive perception of the Act as a deterrent to cybercrime can foster a safer digital environment and promote greater confidence in mobile technology.

The significance of this theme lies in its widespread recognition among participants. The belief that the Act could mitigate digital fraud highlights the public's growing concern over the risks posed by cybercrime in an increasingly connected world. By requiring users to register their SIM cards, the government effectively creates a layer of accountability that did not exist previously. This, in turn, helps people feel more secure when using mobile phones for financial transactions or other sensitive activities. One participant shared, "*With the registration in place, I don't worry as much about getting scammed through SMS or calls*."

Data security concerns. One of the most prominent concerns voiced by participants during the study was centered on data security. The requirement to submit personal information as part of the SIM Card Registration Act raised alarm among participants, who expressed significant fear about the potential misuse or leakage of their sensitive data. As one participant articulated, "*My information might be used for something else*," which encapsulates the widespread anxiety about how this information might be handled after submission. This fear is reflective of broader societal concerns regarding data privacy, especially in contexts where individuals are required to submit personal information to government bodies or third-party organizations. Many participants felt that they lacked control over their data once it was submitted, leading to heightened skepticism about the safeguards in place to protect this information. This skepticism was particularly pronounced among participants who had experienced or were aware of previous incidents where personal data had been compromised. Their concerns are valid, especially given that data breaches involving government institutions have occurred in the past, eroding public confidence in the ability of authorities to protect sensitive information (Chin, 2024).

A sub-theme that emerged from the interviews was the lack of trust in the government's ability to ensure robust data protection mechanisms. Participants were not only concerned about their personal information being used for unintended purposes but also questioned the government’s capability to safeguard sensitive data against breaches. One participant asked, "What if my information is leaked?" This question was particularly common among older participants, many of whom recalled instances where government institutions had been involved in data security failures.

The apprehension regarding government-led cybersecurity practices was not limited to isolated cases but was a recurring theme throughout the discussions. Some participants pointed

to previous data breaches in the Philippines, such as the 2016 hacking of the Commission on Elections (COMELEC) website, which compromised the personal information of millions of registered voters. Such incidents have contributed to a collective memory of vulnerability, making participants question whether the current government has improved its cybersecurity defenses. The persistence of these fears indicates a long-standing distrust in the government's ability to implement effective and secure data protection frameworks.

The findings suggest that public confidence in data security is crucial for the success of policies like the SIM Card Registration Act. To address the concerns raised by participants, it is essential for the government to enhance its cybersecurity infrastructure and adopt transparent measures to reassure citizens about the safety of their data. Public education campaigns that clearly explain the data protection protocols in place and how individuals' information will be used could also help mitigate fears. Additionally, offering options for regular monitoring or data deletion could give individuals more control over their personal information and build greater trust in the system.

Impact on privacy. Another significant theme that surfaced from the study was the perceived loss of personal freedom among participants. Many expressed discomforts with the idea that the SIM Card Registration Act allowed for increased surveillance of their mobile activities. Statements like, "*I feel like my every move is tracked*," reflect these concerns, as participants felt the Act enabled greater government oversight of their personal lives. This sense of being constantly monitored fostered anxiety about their privacy, contributing to the perception that their freedom of movement and communication was being restricted. Participants shared various sources fuelling their belief that SIM registration could lead to increased surveillance and tracking. Some cited news reports and social media discussions that highlighted government surveillance practices, while others pointed to personal experiences, such as targeted ads or messages that seemed to align closely with their recent activities.

This sentiment aligns with existing research that highlights how government policies requiring personal data often evoke concerns about civil liberties. Rowe (2020) noted that data collection practices by governments frequently raise questions about the balance between security and individual freedoms. In this context, participants viewed the mandatory registration as a form of government overreach, fearing that the act could infringe on their right to privacy. These fears suggest that citizens may be more inclined to view policies like the SIM

Card Registration Act as threats to their personal autonomy, even if such policies are designed to enhance security. Notably, these privacy concerns were particularly pronounced among older participants, who may be less familiar with the data collection norms of the digital economy. Unlike younger individuals who have grown up in an era where personal data exchange is commonplace, older participants viewed the Act as an intrusion into personal space. This suggests that age plays a critical role in shaping attitudes toward data collection practices, with older adults perceiving greater risks to their personal freedom because of the Act.

Registration process challenges. The challenges related to the registration process were cited by some participants, who described it as cumbersome and prone to technical issues. Some participants mentioned experiencing delays, which hindered the completion of their registration. "*It was hard to get the confirmation*," one participant explained, noting that these difficulties not only delayed the process but also made it feel unnecessarily complicated. These findings point to a gap between policy formulation and implementation efficiency. While the Act's goals are well-intended, issues related to execution, such as user experience during registration, undermine its potential success. Similar issues in technological rollouts have been documented in other countries where digital transformation programs were implemented without adequate infrastructure (Hendrawan et al., 2023).

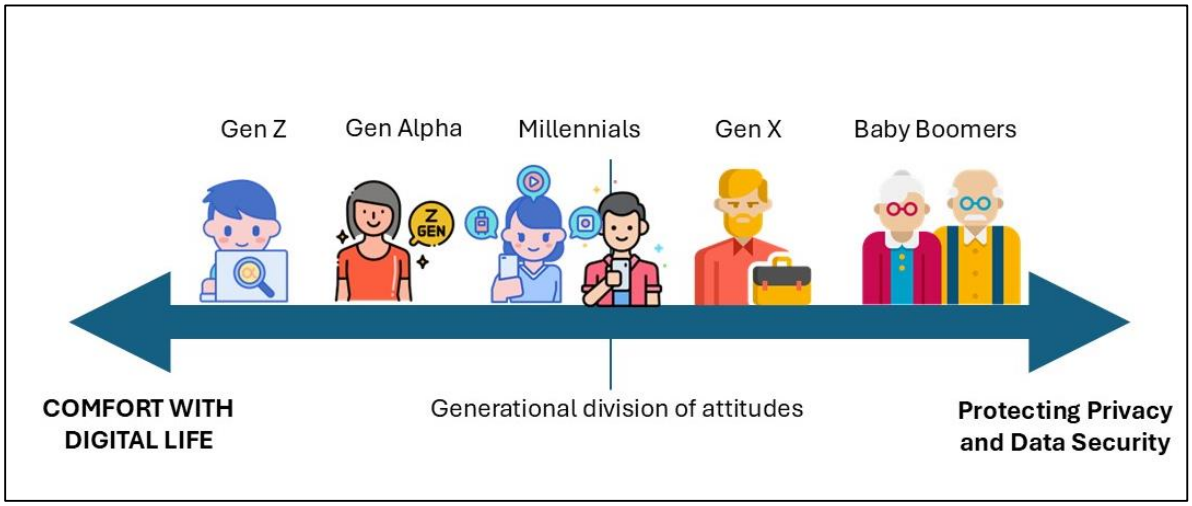
Differing perceptions by age. The study uncovered notable age-related differences in how participants perceived the SIM Card Registration Act, particularly in terms of privacy and data security concerns. These differences were apparent between younger participants, aged 16 to 30, and older participants, aged 31 to 64, highlighting how generational experiences with technology shape attitudes toward government policies involving data collection.

Among younger participants, there was a marked sense of acceptance toward the registration process. This group, raised in a world dominated by smartphones, social media, and various online platforms, seemed to regard data sharing as a routine part of digital life. Statements such as "*It's no big deal for me; everything is online*" reflected a general sense of comfort with the idea that personal information is regularly shared and stored in various digital systems. This attitude aligns with research that suggests digital natives—individuals who have

grown up with the internet—are more accustomed to sharing personal data (DeBrusk & Kreacic, 2023; Anderson & Rainie 2010).

Figure 3

Visual representation of varied perceptions based on generation



***Icon Source**:* Flaticon.com

For this demographic, privacy trade-offs for convenience are seen as part of the online experience. Their familiarity with apps, social media platforms, and e-commerce sites, where data sharing is often a requirement, has normalized the act of providing personal information in exchange for access to services. This reflects a broader trend among younger individuals, who are generally more willing to share personal data if it leads to greater ease in accessing and using digital services (DeBrusk & Kreacic, 2023). Additionally, younger participants appeared to have higher trust in the government's ability to manage and secure their data, possibly influenced by their regular interaction with digital platforms that require similar trust in data handling. In contrast, older participants, aged 31 to 64, displayed a greater degree of skepticism regarding the SIM Card Registration Act. Many in this age group expressed concerns about the long-term implications of data sharing, particularly regarding privacy protection and potential misuse of personal information. One participant remarked, "*Privacy is something we should protect more*," signaling a heightened awareness of the risks associated with personal data exposure.

This generational divide in attitudes toward data privacy is consistent with the article written by Baig (2021), which suggest that older individuals are more likely to prioritize

privacy and express concerns about government or corporate surveillance. For these participants, the SIM Card Registration Act represents a potential invasion of personal privacy, and they are more likely to question the necessity of providing personal data, particularly to government institutions. Their experiences, often informed by instances of data breaches or misuse of information in the past, contribute to a lack of trust in the government's ability to protect their information adequately.

The skepticism among older participants also reflects a broader concern about the expansion of surveillance through digital tools. Many viewed the SIM Card Registration Act as a step toward increased government control, particularly over personal freedoms. This concern is not unique to the Philippines; globally, older populations tend to resist policies that mandate personal data submission, as they perceive such measures as threatening to civil liberties. The difference in technological experience between older and younger generations likely exacerbates this divide, with older participants being less accustomed to the ubiquity of digital systems and the extent of data collection they entail.

The study's findings underline the existence of a generational divide when it comes to attitudes toward privacy and data security. While younger participants seem to accept data sharing as a necessary trade-off for participation in the digital world, older participants view privacy as something that should be more carefully guarded. This divide may stem from different life experiences and exposure to technology. Younger individuals, having grown up in a digitally connected world, tend to have a more utilitarian approach to data sharing, focusing on the convenience it brings. Older individuals, on the other hand, may be more influenced by a history of privacy advocacy and a belief in the importance of keeping personal information secure.

5. Conclusion

Exploring the perceptions among selected residents in San Pablo City, Laguna regarding the implementation of the SIM Card Registration Act through delving into the lived experiences of participants across different age groups, the research revealed critical insights into the perceived effectiveness of the Act, as well as concerns about data security and personal freedom. The findings underscore the complex and multifaceted nature of public reactions to government-mandated data collection policies, with significant implications for both policy implementation and public trust in digital governance.

A key theme that emerged was the perceived effectiveness of the SIM Card Registration Act in preventing mobile-related crimes such as phishing and fraud. Many participants acknowledged that the Act had the potential to deter cybercrime by providing a mechanism for tracking criminal activity through mobile numbers. This view aligns with the government's stated objectives, suggesting that the Act has garnered public support for its role in enhancing national security. However, while participants felt that the Act could help mitigate certain types of crime, there was skepticism about its ability to address more severe threats. This indicates that while the Act may be viewed positively in terms of its immediate goals, its broader effectiveness in ensuring public safety remains a subject of doubt.

Another significant finding relates to data security concerns, particularly among older participants. While younger participants appeared more willing to accept the trade-offs between privacy and convenience in the digital age, older individuals expressed reservations about the long-term use and potential misuse of their personal information. This generational divide highlights the growing anxiety surrounding data privacy in an increasingly connected world. Participants feared that their information could be vulnerable to breaches or misappropriation, with many citing previous incidents involving government institutions as a basis for their concerns. These findings underscore the importance of trust in government data handling practices, especially when it comes to sensitive personal information.

In tandem with data security concerns, the perceived loss of personal freedom was another major theme. Participants, particularly from older age groups, expressed discomfort with the notion that the Act facilitated government surveillance of their mobile activities. They viewed the Act as a potential infringement on their civil liberties, expressing fears that it could lead to a loss of autonomy. This sentiment resonates with broader concerns about government overreach, particularly in policies that mandate the collection of personal data. The sense of being constantly monitored heightened participants' anxieties about the erosion of personal privacy, suggesting that the Act’s implementation may have unintended consequences for how individuals perceive their relationship with the state.

Notably, the study revealed age-related differences in attitudes toward the Act. Younger participants, who are more accustomed to the ubiquity of data sharing in social media and digital services, were less concerned about privacy issues. They generally viewed the registration process as a standard requirement for participation in a digitally connected world, and many expressed a willingness to trade off privacy for convenience. In contrast, older

participants displayed greater caution and skepticism. They were more likely to question the necessity of the Act, viewing it as an intrusion into personal space and a threat to privacy. This generational divide is significant, as it points to differing levels of trust in digital governance based on technological familiarity and life experience.

The findings of this study can contribute to the enhancement of SIM Card Registration Act policies and their implementation in several ways. First, policymakers should develop targeted communication strategies that address the specific concerns of different age groups. For older participants, emphasizing data security measures and privacy protections may alleviate fears about personal information misuse. For younger individuals, highlighting the convenience and security benefits of registration can foster a more positive perception. Additionally, enhancing data protection measures and providing transparency about how personal information is handled can build public trust. Regular audits and independent assessments of data handling practices can further assure residents of the government's commitment to safeguarding their information. Increasing public engagement and education on the SIM Card Registration Act can address misconceptions and foster a better understanding of the law's objectives. Lastly, establishing channels for continuous feedback from the public on the implementation of the Act can help policymakers identify areas for improvement and adapt the law to better meet the needs and concerns of the community. With these, the SIM Card Registration Act can become more effective in achieving its objectives while fostering public trust and cooperation.

To enhance the significance of future research on the SIM Card Registration Act and its impact on crime prevention, it is recommended that studies incorporate qualitative interviews with individuals who have directly experienced criminal activities related to mobile communication, such as phishing, fraud, or harassment. Gathering firsthand accounts from victims who navigated the legal processes established by the Act can provide invaluable insights into the effectiveness of the law in addressing their concerns. This approach could illuminate the challenges and successes faced by individuals in resolving these issues and highlight the Act's real-world implications on public safety and security. Furthermore, exploring participants' perceptions of their experiences with law enforcement and the legal system can enrich the understanding of the Act's role in fostering trust and efficacy in governmental responses to digital crimes. Such studies could lead to actionable

recommendations for improving the law and enhancing public awareness, ultimately contributing to a more robust framework for addressing mobile-related crimes.

Disclosure statement
No potential conflict of interest was reported by the author(s).

Funding
This work was not supported by any funding.

ORCID
Aera L. Diaz – https://orcid.org/0009-0009-3157-4270

Romano M. Balbacal – https://orcid.org/0000-0002-0817-203X

References

Ahmad, T. (2020). Student perceptions on using cell phones as learning tools. *PSU Research Review*, *4*(1), 25–43. https://doi.org/10.1108/prr-03-2018-0007

Airalo (2022, April 29). The top 10 problems with SIM cards. Airalo. https://www.airalo.com/blog/the-top-10-problems-with-sim-cards

Ahmed, S. I., Haque, M. R., Guha, S., Rifat, M. R., & Dell, N. (2017). Privacy, security, and surveillance in the global south. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 906–918. https://doi.org/10.1145/3025453.3025961

Ahmed, S. I., Haque, M. R., Haider, I., Chen, J., & Dell, N. (2019). Everyone has some personal stuff. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 180, 1-13. https://doi.org/10.1145/3290605.3300410

AlMarshoud, M., Kiraz, M. S., & Al-Bayatti, A. H. (2024). Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. *ACM Computing Surveys*, *56*(10), 1-39. https://doi.org/10.1145/3656166

Anderson, J., & Rainie, L. (2010). Millennials will make online sharing in networks a lifelong habit. Pew Research Center. https://www.pewresearch.org/internet/2010/07/09/millennials-will-make-online-sharing-in-networks-a-lifelong-habit/

Baig, E. (2021). Older adults wary about their privacy online. *AARP*. https://www.aarp.org/home-family/personal-technology/info-2021/companies-address-online-privacy-concerns.html

Birkland, T. A. (2019). *An introduction to the policy process.* Routledge. https://doi.org/10.4324/9781351023948

Bischoff, P. (2023). Which governments impose SIM-card registration laws to collect data on their citizens? *Comparitech.* https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/

Blancaflor, E., Calberto, D., Lara, C., & Mancilla, D. F. (2024). Guarding against phone scammers: An examination of gaining access to phone contacts through smishing social engineering exploits. *Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence*, 365-372.

Bowyer, C., & Bowyer, C. (2023). Navigating the threat of SIM swap fraud. *Onfido.* https://onfido.com/blog/sim-swap-fraud/

Cabalza, D. (2022, October 12). PNP: 'More teeth' vs online crimes with SIM card law. *INQUIRER.net.* https://newsinfo.inquirer.net/1678579/pnp-more-teeth-vs-online-crime-with-sim-card-law

Chi, C. (2023). More than half of Philippine SIMs already registered before July 25 deadline — DICT. *Philstar.com.* https://www.philstar.com/headlines/2023/07/25/2283694/more-half-philippine-sims-already-registered-july-25-deadline-dict

Chin, K. (2024). Biggest data breaches in US history. *Upgard.* https://www.upguard.com/blog/biggest-data-breaches-us

De Brusk, C., & Kreacic, A. (2023). How Gen Z uses social media is causing a data privacy paradox. *Oliver Wyman Forum.* https://www.oliverwymanforum.com/gen-z/2023/aug/how-gen-z-uses-social-media-is-causing-a-data-privacy-paradox.html

Galvan, A. (2019). The unrested adolescent brain. *Child Development Perspective, 13*(3), 141-146. https://doi.org/10.1111/cdep.12332

Gonzales, S. M., & Villacruel, P. D. (2024). Exploring students' experiences in the dynamic learning program model. *International Journal of Educational Management and Development Studies, 5*(2), 1-26. https://doi.org/10.53378/353051

Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y. C., & Mejía, D. D. (2021). Evaluating criminal transactional methods in cyberspace as understood in an international context. *Flinders University Research Repository*. https://researchnow.flinders.edu.au/en/publications/evaluating-criminal-transactional-methods-in-cyberspace-as-unders

GSMA. (2021). Access to mobile services and proof of identity 2021. https://www.gsma.com/mobilefordevelopment/resources/access-to-mobile-services-and-proof-of-identity-2021/

Hendrawan, S. A., Chatra, A., Iman, N., Hidayatullah, S., & Suprayitno, D. (2024). Digital transformation in MSMEs: Challenges and opportunities in technology management. *Jurnal Informasi dan Teknologi*, 141-149.

Howlett, M. (2018). Moving policy implementation theory forward: A multiple streams/critical juncture approach. *Public Policy and Administration, 34*(4), 405–430. https://doi.org/10.1177/0952076718775791

Kanishka. (2023, June 11). Advantages of using mobile phone over landline phones. *Airtel.* https://www.airtel.in/blog/prepaid/advantages-of-mobile-over-landline/

Kim, I., Kim, R., Kim, H., Kim, D., Han, K., Lee, P. H., Mark, G., & Lee, U. (2019). Understanding smartphone usage in college classrooms: A long-term measurement study. *Computers & Education, 141*, 103611. https://doi.org/10.1016/j.compedu.2019.103611

Kim, M., Suh, J., & Kwon, H. (2022, August). A study of the emerging trends in SIM swapping crime and effective countermeasures. In *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)* (pp. 240-245). IEEE. https://doi.org/10.1109/BCD54882.2022.9900510

Khalili, N. (2022). *Design and implementation of a blockchain-based global authentication system using biometrics and subscriber identification module* (Doctoral dissertation, Université d'Ottawa/University of Ottawa). http://dx.doi.org/10.20381/ruor-27891

La Torre, G., De Leonardis, V., & Chiappetta, M. (2020). Technostress: How does it affect the productivity and life of an individual? Results of an observational study. *Public Health, 189*, 60–65. https://doi.org/10.1016/j.puhe.2020.09.013

Luna, E. (2023). Failure to comply with July 25 SIM card registration deadline will risk customers to permanent cancellation of mobile services as well as communication

disruption. *Manila Bulletin.* https://mb.com.ph/2023/7/24/failure-to-comply-with-july-25-sim-card-registration-deadline-will-risk-customers-to-permanent-cancellation-of-mobile-services-as-well-as-communication-disruption

Lu, D., Guo, F., & Li, F. (2020). Evaluating the causal effects of cellphone distraction on crash risk using propensity score methods. *Accident Analysis and Prevention, 143,* 105579. https://doi.org/10.1016/j.aap.2020.105579

Manticajon, I. (2023, July 31). SIM card registration: A double-edged sword? *Philstar.com.* https://www.philstar.com/the-freeman/opinion/2023/08/01/2285375/sim-card-registration-double-edged-sword

Marks, G. (2021, September 19). 'Smishing': The rising threat for business owners that brings scams to smartphones. *The Guardian.* https://www.theguardian.com/

Miller, A. B., Sears, M. E., Morgan, L. L., Davis, D. L., Hardell, L., Oremus, M., & Soskolne, C. L. (2019). Risks to health and well-being from radio-frequency radiation emitted by cell phones and other wireless devices. *Frontiers in Public Health, 7,* 223. https://doi.org/10.3389/fpubh.2019.00223

Mugambwa, J., Nabeta, I. N., Ngoma, M., Rudaheranwa, N., Kaberuka, W., & Munene, J. C. (2020). Policy implementation: A review of selected literature. *System Dynamics for Performance Management,* 91–116. https://doi.org/10.1007/978-3-030-42970-6_5

Privacy International. (2022, May 16). Timeline of SIM card registration laws. https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws

Republic Act No. 11934: Subscriber Identity Module (SIM) Registration Act. (2022). lawphil.net. https://lawphil.net/statutes/repacts/ra2022/ra_11934_2022.html

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management, 55,* 102178. https://doi.org/10.1016/j.ijinfomgt.2020.102178

Sabatier, P. A. (2019). Fostering the development of policy theory. In Routledge eBooks (pp. 321–336). https://doi.org/10.4324/9780367274689-11

Salem. (2021). *Implementing public policy.* Salem Word Press.

Wanja, G. M. (2021). *A prototype to identify fraudulent SIM card registration using public key infrastructure verification approach* [Thesis, Strathmore University]. http://hdl.handle.net/11071/12915