A MEMORANDUM AFFIRMING THE UNCONSTITUTIONALITY OF REPUBLIC ACT NO. 11934, OTHERWISE KNOWN AS THE SUBSCRIBER IDENTITY MODULE (SIM) REGISTRATION ACT, AND NATIONAL TELECOMMUNICATIONS COMMISSION MEMORANDUM CIRCULAR NO. 001-12-2022, OR THE RULES AND REGULATIONS IMPLEMENTING REPUBLIC ACT NO. 11934

Submitted to:
KIRK YNGWIE MONTUERTO ENRIQUEZ

Submitted by:
Aya-ay, Raymond Anthony P. (Assistant Researcher)
Balaga, Darcy Leonard V. (Assistant Researcher)
Barcenilla, Jomer Allan G. (Assistant Researcher)
Dayata, Wayne Matthew A. (Oralist Speaker)
Kuizon, Joshua R. (Assistant Researcher)
Labana, Hannah Ruth B. (Assistant Researcher)
Leaño, Jomar M. (Assistant Researcher)
Monzales, Kathleen Iza M. (Rebuttalist Speaker)
Orbiso, Josh Arkane C. (Assistant Researcher)
Robles, Nhemuel B. (Closing Arguments Speaker)
Rosales, Jade Andrie T. (Assistant Researcher)
Sucalit, Giovanni Ross P. (Head Researcher)
Tugonon, Francis V. (Assistant Researcher)
Valeros, Marc Nathaniel (Assistant Researcher)

May 3, 2023

TABLE OF CONTENTS

INDEX OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

FOREWORD

Republic Act No. 11934, otherwise known as the "Subscriber Identity Module (SIM) Registration Act"[1], is a law signed by President Ferdinand Marcos Jr. last October 10, 2022 and taken into effect last October 27, 2022, which has been recently implemented nationwide and across all Public Telecommunication Entities (PTEs). Section 2 of the Republic Act No. 11934 states its declaration of policy which serves as the core purpose of the law:

> "The State recognizes the vital role of information and communications technology in nation-building and encourages its growth and development.
>
> It is equally cognizant that as beneficial as modern technology is, its illegal or malicious use endangers people's lives, damages property, poses hazards to public order, and even threatens the security of nations.
>
> The State shall promote responsibility in the use of Subscriber Identity Module (SIM) and provide law enforcement agencies the tools to resolve crimes which involve its utilization and a platform to deter the commission of wrongdoings."

Section 4 of R.A. No. 11934 introduces the system of mandatory registration of SIM cards as a prerequisite to its activation. All SIMs to be sold by PTEs or resellers shall be in a deactivated state until the purchaser of the SIM has successfully registered in compliance with the law. In addition, all existing subscribers should register their SIMs with their respective PTEs within one hundred eighty (180) days from the effectivity of the law, which may be extended by the Department of Information and Communications Technology (DICT) for a period not exceeding one hundred twenty (120) days. Failure to register the existing SIM shall result in the automatic deactivation of the SIM, which may only be reactivated after registration.

The Implementing Rules and Regulations of the SIM Registration Act have been provided by the National Telecommunications Commission (NTC) Memorandum Circular No. 001-12-2022, which was released on December 12, 2022 and began its effectivity on December 27, 2022, the first day of the 180-day allocated duration as stated in the Act.

As of April 24, 2023, 82,845,397 subscribers have registered their SIM, or equivalent to 49.31 percent of the 168 million subscriber base nationwide[2]. Moreover, on April 25, 2023, the DICT has extended the deadline of the SIM registration from the original 180-day deadline of April 26, 2023 for an additional

---

[1] Republic Act No. 11934 (October 10, 2022) (Phil.)
[2] Garcia, J. F., & Tamayo, B. E. (2023, April 24). DICT to extend SIM card registration deadline. The Manila Times. https://www.manilatimes.net/2023/04/25/news/national/dict-to-extend-sim-card-registration-deadline/1888579

90 days or until July 25, 2023, citing that there has to be a boost of information dissemination and reach to broaden the awareness of this Act to the rest of the Filipinos especially those with limited to no mobile data access to perform the registration[3].

Despite the law being enacted, there are several privacy issues that were put forward for discussion among the community but were still not resolved, thus leading to the low number of registrants due to citizens still being highly concerned about the safety and security of the implementation of the said Act, particularly on the transmitting and storing of data on the databases of the PTEs. In fact, a similar bill was initially passed in the 18th Congress but was vetoed by then-President Rodrigo Duterte on April 14, 2022 due to the inclusion of social media accounts, which Duterte "was constrained to disagree" with as it may "give rise to a situation of dangerous state intrusion and surveillance threatening many constitutionally protected rights"[4].

One of the primary concerns is the constitutionality of the mandatory SIM registration requirement. The Philippine Constitution guarantees the right to privacy of communication and correspondence, which includes the right to keep one's mobile number private. The mandatory SIM registration requirement poses a threat to this right by compelling individuals to disclose their personal information, including their full name, address, date of birth, and government-issued ID number, among others.

Moreover, there have been numerous reports of data breaches and leaks involving the personal information of Filipinos, including those who have registered their SIMs. These incidents have raised concerns about the adequacy of measures taken by telecommunication companies and government agencies to protect the personal data of citizens. In light of these issues, it is crucial to evaluate the constitutionality of the mandatory SIM registration requirement and its implications on the right to privacy of Filipinos.

This memorandum aims to examine the legal issues surrounding the mandatory SIM registration requirement under the SIM Registration Act and its Implementing Rules and Regulations and its potential impact on the right to privacy. It will explore the constitutionality of the requirement in light of the guarantees provided by the Philippine Constitution and the data privacy laws in the Philippines, as well as the implications of data breaches and leaks on the privacy of Filipinos. Through this memorandum, we hope to shed light on the legal issues and concerns surrounding the mandatory SIM registration requirement and provide recommendations for addressing them.

---

[3] Pulta, W. B. a. B. (2023, April 25). SIM card registration extended for 90 days. Philippine News Agency. https://www.pna.gov.ph/articles/1200057

[4] Mercado, N. A. (2022, April 15). "Duterte vetoes SIM Card Registration bill". Inquirer News.. https://newsinfo.inquirer.net/1583318/fwd-duterte-vetoes-sim-card-registration-bill

LEGAL ISSUE

Republic Act No. 11934, otherwise known as the Subscriber Identity Module (SIM) Registration Act, and National Telecommunications Commission Memorandum Circular No. 001-12-2022, or the Rules and Regulations Implementing Republic Act No. 11934, are unconstitutional for being violative of the right to privacy under Section 3(1), Article III of the 1987 Constitution, and are inconsistent with the provisions of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 and its Implementing Rules and Regulations.

SUMMARY OF ARGUMENTS

The State's pursuit of promoting responsible usage of the Subscriber Identity Module (SIM), and its efforts to create tools for law enforcement agencies to utilize in resolving crimes and deter wrongdoings, there are aspects that need to be addressed before we can fully determine the constitutionality of Republic Act No. 11934 or the Subscriber Identity Module Registration Act.

The SIM Registration Act can lead to increasingly critical and devastating cybercriminal acts. While this act aids in the resolution and deterrence of crimes, it also invites cybercriminals to create more cunning ways to access sensitive personal information. Even with this act in place, the government's and the PTE's (Public Telecommunications Entities) cybersecurity measures are not sufficient to ward off cybercrime.

The SIM Registration Act is in conflict with the implementation rules and regulations of The Data Privacy Act of 2012. The registration of end-users has excessive unnecessary requirements, forces consent for the collection of sensitive personal information and proves to be ineffective in protecting the life and health of data subjects. The requirement for facial recognition or biometric information to register a SIM is excessive and goes beyond what is required by law. This is in violation of Section 11 of the DPA which requires that personal information be collected and processed in compliance with the Act's requirements. This requirement deprives citizens of the right to secure sensitive information and is ultimately not essential in curbing cybercrime. The potential for nationwide breaches and the resulting consequences are severe and irreversible.

There exists the potential of the government to over-surveil. The SIM Registration Act gives way for the government to suppress target individuals given the data that they are provided as mandated by this act. This can lead to abuse of power, corruption, and violation of human rights.

There is a potential for loss of data control on end users. There have been instances where sensitive data was compromised in an unprecedented data breach. Data breaches are costly and devastating when they happen to corporate entities, and even more so when it happens to government agencies that hold sensitive data of millions of citizens.

The SIM Registration Act creates an additional means of unlawful data usage. The NTC recently allowed PTEs to use the data collected from the SIM registration for marketing purposes. This raises questions about how the gathered data is being used. Furthermore, authorities may be able to track an individual's location and movements through their SIM card, leading to surveillance and the creation of a detailed profile of their daily activities and interests. There is also a risk of identity theft on SIM replacement associated with mandatory SIM card registration.

Having access to SIM cards and users' information, PTEs can gather information on the users' online activity, places visited, and real-time locations. While there are requisites to access the information of users, there are still ways that people in power can circumvent these.

Other threats and dangers to registered SIM card holders: PTEs could employ third-party contractors to store the collected data from the SIM Registration Act. These contractors may originate from countries whose data privacy laws may not coincide with the Philippines' Data Privacy Act of 2012. This may allow them to sell or manipulate the data that they are holding.

ARGUMENTS

A. SIM Registration can lead to increasingly critical cybercriminal acts

The process of connecting a mobile phone number to the identification of its user is known as SIM card registration. SIM card registration's main objective is to enhance security and stop illegal actions like fraud, terrorism, and other crimes that can be made easier by anonymous communication. Although it has positive effects, it may also lead to unintended consequences.

In compliance with the SIM registration act, we are mandated to provide personal and sensitive information such as our full name, current address, valid identification cards, and even facial recognition data. However, the provision of this personal and sensitive information poses significant risks in terms of cybersecurity. The collection and storage of this information can increase the likelihood of cybercriminal acts such as text phishing, identity theft, data hacking, data loss and data breach.

Text phishing, identity theft, data hacking, data breaches, and other criminal acts are still prevalent despite some countries have already implemented mandatory registration of SIM cards and increased their cybersecurity which implies that the SIM registration act does not guarantee protection against cyber-criminal acts.

Such as in Indonesia on August 31, 2022, A hacker named Bjorka, leaked 1.3 billion sim registration details and listed them for sale on a dark web online marketplace. This data leak revealed national identity numbers, phone numbers, and more. Making it very alarming since the hacker did not just steal information from telecommunication companies but also from the government. The hacker’s intent in leaking that data is to show how weak the government's cybersecurity is.[5]

Also in February 2022, Australian telecommunications company Optus reported that it had suffered a data breach, which resulted in the theft of personal data belonging to millions of its customers. The company revealed that the hackers were able to access and exfiltrate a vast amount of customer data, including their full names, birthdates, home addresses, phone and email contacts, and even passport and driving license numbers. Optus did not disclose how many customers were affected, but reports suggest that the breach could have compromised the personal data of millions of people. [6]

---

[5] Auto, H. (2022, September 19). Indonesia hunts for Bjorka, hacker selling 1.3b SIM card users' data, taunting officials. The Straits Times. https://www.straitstimes.com/asia/se-asia/indonesia-hunts-for-bjorka-hacker-selling-13b-sim-card-users-data-taunting-officials

[6] Doherty, B. (2022, September 22). Customers' personal data stolen as Optus suffers massive cyber-attack. The Guardian. Retrieved May 3, 2023, from https://www.theguardian.com/business/2022/sep/22/customers-personal-data-stolen-as-optus-suffers-massive-cyber-attack

The data breach serves as a reminder that Public telecommunication entities (PTE) are prone to cyberattacks and it exposes the danger that customers encounter when confiding their personal information to these firms. Given its stature as one of Australia's telecommunication giants, Optus should have implemented strong cybersecurity protocols to protect its customers' information. However, the data breach suggests that even the most advanced security measures can be penetrated by resolute cybercriminals.

The data breach of Optus and the government of Indonesia raises serious concerns about the trustworthiness of PTEs and the government and their ability to protect their customers' sensitive data. Customers rely on them to ensure the confidentiality and integrity of their personal information. But because of these circumstances, people are questioning whether we can also trust the Philippine government and the PTEs of the country in safeguarding our personal data, especially since the Philippine government is known to be repressive.

Furthermore, scammers and cybercriminals can be very creative in finding ways to circumvent SIM registration and other cybersecurity measures. They may use spoofing or VPNs to easily hide their identities and avoid being identified by the government, indicating that the cybersecurity of the government and the PTE are not that effective or sufficient to combat cybercrime. According to Sen. Grace Poe (2023), "There are still SIM farms out there and spoofing tools. Sinister minds will never stop hatching ways of stealing information and duping people".[7]

Despite the ongoing SIM registration act, text scams are still rampant, showing that cybersecurity of the government and the public telecommunications entities (PTE) are not yet foolproof. In fact, a very recent news article stated that over 1 million records from NBI, PNP, and other agencies leaked in a massive data breach. A staggering 1,279,437 records belonging to law enforcement agencies, including sensitive police employee information, have been compromised in an unprecedented data breach, as revealed by a report from the leading cybersecurity research company VPNMentor on Tuesday (April 18, 2023).[8]

While it is true that having one's SIM registered SIM can help identify theft and fraud by permitting law enforcement agencies to verify suspicious users and track their activities, it is also true that not all cybercriminals can be easily identified and tracked through SIM registration. By simply not registering their SIMs, they cannot be tracked especially whenever they commit crimes on data breach. They may use spoofing or VPNs to easily hide their identities and avoid being identified by the government. This becomes more challenging to identify and track cybercriminals because they can use different tactics to avoid being caught

[7] Poe: Text scams still rampant despite ongoing SIM registration. (2023, March 19). CNN Philippines. Retrieved May 3, 2023, from http://www.cnnphilippines.com/news/2023/3/19/poe-text-scams-rampant-sim-registration.html

[8] Abrogar, S. (2023, April 19). Over 1M records from NBI, PNP, and other agencies leaked in a massive data breach. Inquirer.net. Retrieved May 3, 2023, from https://newsinfo.inquirer.net/1758456/over-1-million-records-from-nbi-pnp-other-agencies-leaked-in-huge-data-breach

through registered SIMs. This emphasizes that SIM registration does not totally protect people from cybercrimes since criminals can employ other tactics that can avoid being found through SIM registration, however, this situation raises concerns among citizens regarding their confidence in the government's ability to safeguard their personal information.

B. Conflict of the Implementation Rules and Regulations of Subscriber Identity Module (SIM) Registration Act with the Data Privacy Act of 2012

Republic Act No. 10173, more commonly referred to as the Data Privacy Act of 2012, was enacted with the singular objective of safeguarding the fundamental human right to privacy of information, while simultaneously facilitating the unobstructed transmission of information to stimulate innovation and foster growth. This law recognizes the crucial role played by information and communication technologies in the development of the nation and therefore imposes a duty on the State to ensure that the confidentiality, integrity, and availability of personal data within government and private sector information systems are adequately protected. The Data Privacy Act of 2012 mandates that all entities engaged in the collection, processing, and storage of personal data adhere to strict standards and principles aimed at preserving the privacy and security of such information. Section 4 provided the scope of the act which includes processing of all types of personal information and to all natural and juridical persons involved in personal information processing, including those using equipment located in the Philippines or maintaining an office, branch, or agency in the country.

The State also recognizes its inherent responsibility to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected. The National Privacy Commission (NPC) was established to administer and implement the provisions of the Act and to monitor and ensure compliance of the country with international standards set for data protection. Furthermore, the NPC performs several significant functions, including rule-making, advisory services, public education, compliance and monitoring, management of personal data processing systems registration, complaint investigation, and law enforcement.

In an article regarding the Subscriber Identity Module (SIM) Registration, the NPC warned that there are risks that may arise due to overcollection and improper or inadequate monitoring practices. The commission stated that retailers may lack the necessary skills and resources to confirm identities and authenticate ID cards.[9] Additionally, Computer Professionals Union (CPU) Secretary-General, Kim Cantillas, stated that such implementation would jeopardize the people knowing the inadequate enforcement of the Data Privacy Act (DPA) and the lack of awareness among the population regarding our entitlement to privacy which represents an added peril to individuals. As part of the efforts to mitigate cyber scams, the government is considering the implementation of mandatory registration for sim cards. On September 28, the House of Representatives granted approval for House Bill No. 14, which requires the registration of both pre-existing and newly acquired SIM cards. The aforementioned bill was authored by the honorable House Speaker Martin Romualdez, along with Representatives Ferdinand Alexander

[9] Rappler. (2022b, October 8). NPC cites ways to shield SIM card registration from data breaches. *RAPPLER*.https://www.rappler.com/nation/national-privacy-commission-ways-shield-sim-card-registration-security-risks/

Marcos, Yedda Marie Romualdez, and Jude Acidre. Subsequently, on October 10, the bill was signed into law by President Ferdinand "Bongbong" Marcos Jr as Republic Act No. 11934, otherwise known as the SIM Registration Act or the Subscriber Identity Module Registration Act.[10]

Republic Act No. 11934 requires all SIM cards to be registered with their respective Public Telecommunications Entity (PTE) or telecommunication companies within one hundred eighty (180) days from the effectivity of this Act. Failure to do so will result in the deactivation of their SIM cards. It provides the following guidelines for subscribers when registering their SIM cards: (1) registration form with their full name, date of birth, sex, and address; (2) presentation of any valid government identification cards (ID); (3) input of the assigned mobile number of SIM; (4) registration of a SIM card by a minor under the name of their parents and guardians; and (5) registration by foreigners to use SIM cards with temporary validity.[11]

The requirement for facial recognition or any biometric information to register a SIM is unnecessary because of its inherent excessiveness that goes beyond the adequacy required by the law as specified in Section 11 of the DPA which describes how personal information must be collected and processed in compliance with the requirement of Act. The fourth provision of the said section stated that personal information must be adequate and not excessive in relation to the purposes for which they are collected and processed. Consequently, the collection of such information deprives the citizen of the right to secure intimate and sensitive information that is, ultimately, not essential in the attempts of curbing cybercriminal activities. The possibility of nationwide breaches, for individuals and organizations alike, and the drastic consequences that they might incur are irreversibly devastating.[12]

The Data Privacy Act of 2012 allows the processing of sensitive personal information and privileged information as long as the protection is guaranteed and the consent of the data subjects, which are the SIM card holders in this case, is not required by law.[13] For the SIM Registration Act, all end-users are required to provide their complete name, birth date, sex, address, and valid government-issued IDs which may be considered sensitive personal information. Though it is not required for all individuals to secure a SIM card, it is a crucial daily item of communication. Without it, individuals are not able to connect to local telecommunication networks and communicate with their loved ones and emergency contacts. Failure to register one's SIM cards will result in deactivation, and consequently, getting disconnected.[14] Because of this they are forced to provide

[10] Yuvallos, A. (2022, October 10). The sim card registration law could be a huge security risk. Here's why. *NOLISOLI*. https://nolisoli.ph/104058/sim-card-law/
[11] Republic Act No. 11934, § 5
[12] Hersey, F. (2023, January 13). Pushback against SIM registration in Philippines as India adds facial recognition checks. Biometric Update|. https://www.biometricupdate.com/202301/pushback-against-sim-registration-in-philippines-as-india-adds-facial-recognition-checks
[13] Republic Act No. 10173, § 13(b)
[14] Republic Act No. 11934, § 4

their sensitive personal information to activate their SIM cards just because an individual wants to be in touch with their friends and family. This is not what defines the consensual submission of sensitive personal information. The SIM Registration Act indirectly requires the consent of all end-users to provide their sensitive personal information. Therefore, the collection and processing of personal data as required by the SIM Registration Act are in conflict with the guidelines of sensitive personal information collection in the Data Privacy Act of 2012.

Additionally, Section 13 (c) of the Data Privacy Act of 2012 specifies that the processing of information is necessary to protect the life and health of the data subject or another person, provided that the data subject is not legally or physically able to express consent prior to processing. Ironically, while these attempts at protecting individuals' lives may be commendable, they may be invalidated by the presence of possible data breaches that can have significant consequences on the quality of life of those affected. Although guidelines exist regarding these breaches, there is no ultimate guarantee that they are effective and carried out efficiently. [15]Consequently, Section 13 (d) expresses the same sentiment regarding the quality of life and interests of the data subject, which brings us back to the same argument regarding the effectiveness of established guidelines set out in Republic Act No. 11934. Moreover, it has been pointed out that personal information processing should be carried out by information controllers or any third parties for legitimate purposes, provided it does not override the fundamental rights and freedoms of the data subject or individual, which necessitate protection under the Philippine Constitution. [16] The SIM Registration Act does not provide assurance in securing the rights and freedoms of end-users, therefore, information collected for the purpose of this act should not be mindlessly handled by information controllers or third parties. In this case, the involved PTEs and the Department of Information and Communications Technology should not be able to freely access such sensitive information about the data subjects.

[15] Republic Act No. 10173, § 13(c)
[16] Ibid, § 13(d)

C. Potential Government Over Surveillance and Loss of Data Control on End Users

RA. 11934 forces the end-users to trade in their right to privacy for freedom of speech. It requires subscribers to essentially disclose important and identifying information regarding a person to perform their basic acts of communication such as text messaging and voice calls.

Article III Section 3(1) of the 1987 Philippine Constitution states that "The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law."[17]

Furthermore, under Article II Section 2 of the Constitution, the Philippines adopts generally accepted principles of international law as part of the law of the land.[18] According to Article 12 of the Universal Declaration of Human Rights that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[19]

The protection of personal information on one's health, finances, gender, legal situation, political ideologies, and other factors falls under the right to privacy. It defends people from political persecution, potential hate crimes, and prejudice. It is a constitutional right for everyone to have their information kept private, and to be protected by unlawful and unreasonable search and seizures. The premise of the act is indeed noble: To curb and deter the advances, growth, and illegal activities of scammers. But the means to that end must not come at the price of the privacy rights of the citizens.

In a world run by the internet and gadgets, most if not all Filipino cellphone users are almost always connected to the internet through mobile data when they’re up and about, which cannot be done unless one has a SIM card, or in this era, a registered one. It is no longer reasonable to expect a person to just refuse to get a SIM card to protect the constitutional right to privacy as the world we live in right now makes it almost impossible to not have one.

Under Sections 9 and 10 of R.A. No. 11934, all information obtained during the registration process shall be absolutely confidential. However, disclosure of the full name and address of an end-user shall be made only in four (4) instances: (a) in compliance with any law obligating the PTE to disclose such information in accordance with the Data Privacy Act; (b) in compliance with a court order or legal process upon finding of probable cause; (c) upon the issuance of a subpoena by competent authority based on a sworn complaint that a specific mobile number was or is being used in the commission of a crime or that it was utilized as a means to

[17] 1987 Philippine Constitution, Article III, § 3. (Phil.)
[18] Ibid, Article II, § 2.
[19] Universal Declaration of Human Rights (1948).

commit a malicious, fraudulent, or unlawful act, and that the complainant is unable to ascertain the identity of the perpetrator; or (d) with the written consent of the subscriber.

Government Surveillance

The right to privacy is violated when personal information must be provided to the government and private organizations. It will be simpler for the government and large private organizations such as Telecommunications companies to get, compile, and use all internet and smartphone users' personal information. This includes text messages, social media posts, geo-tagged locations, and other data stored on a cellphone. Such details can be used to profile targets for suppression as well as for commercial advertising.

The SIM card registration will facilitate the spread of misgovernment and maladministration which can lead to government corruption, abuse of power by state agents, police and military crimes, violation of human rights and international humanitarian law, corporate abuse, and environmental destruction. Thus, will create fear and silence for the people as people become hesitant to report abuse, having prior knowledge that they can be traced as the source of the information and can be retaliated against.

It is a way of removing or lessening what is left of the limited democratic space. The state will use this as a tool for intelligence and surveillance to forcefully suppress individuals, organizations, and movements that fight for their rights and strive for change. Furthermore, it will result in many people, particularly the toiling masses who have no or limited access to telecommunications services, being completely deprived of these services.

The Philippines has several intelligence agencies and concerns have been raised by the lack of transparency and oversight of these agencies.[20] There is a lack of oversight mechanisms to monitor the mandate and actions of these agencies. The President, who is the highest authority on national security matters and to whom most agencies report directly, chairs the National Security Council. The Council provides advice to the President on how to integrate various policies related to national security, including domestic, foreign, military, political, economic, social, and educational policies. The absence of mechanisms to oversee these agencies may have an impact on privacy rights. Privacy is a fundamental human right that is essential for protecting human dignity and is the foundation of any democratic society. It also reinforces other rights, such as freedom of expression, information, and association.

[20] Domingo, F. C. (2014). Philippine Intelligence Community: A Case for Transparency. Ateneo de Manila University.
https://www.academia.edu/6704814/Philippine_Intelligence_Community_A_Case_for_Transparency

Lack of Data Control and Security

Government agencies that collect and process personal data remain unregulated because they are exempt from the scope of application of the Data Privacy Act, this implies that the security measures in place to protect against data breaches for large amounts of personal data collected and processed by public bodies are inadequate. As a result, there have been several instances of data breaches over time.[21]

There have been many instances of data leaks from our government's own data bank. What is the assurance that this will not be one of the leaks in the future? Additionally, the Philippine government is no stranger to a lack of data control and security such as in the case of the COMELEC breach which leaked online the personal information of approximately 55 million registered Filipino voters. While some data, such as names, birth dates, and Voter's Identification Numbers were encrypted, other information such as residential address and birthplace were not and could be easily determined. For overseas Filipino voters, details such as birthplace, passport number, and names of parents could be identified by anyone who knew the individual's real name. The risk posed by this breach is immense and cannot be understated. Recognized as one of the largest breaches of government data in history, it highlighted the amount of personal information collected and held by Philippine government agencies and their inability to secure it.[22] With the active and continuous threat of things like red-tagging, it is almost impossible to feel safe knowing that the one main mode of communication that every Filipino has can be used to invade their own privacy so easily with this Act.

Furthermore, 1,279,437 records belonging to law enforcement agencies, including sensitive police employee information, have been compromised in an unprecedented data breach.[23] The huge data breach exposed 817.54 gigabytes of records from multiple state agencies, including the Philippine National Police (PNP), National Bureau of Investigation (NBI), Bureau of Internal Revenue (BIR), and Special Action Force (SAF), putting the personal information of millions of Filipinos at risk. The exposed records included highly sensitive information such as fingerprint scans, birth certificates, tax identification numbers (TIN), tax filing records, academic transcripts, and even passport copies.

Creating a database of individuals' mobile numbers can hinder their ability to communicate privately, increase the likelihood of being tracked and monitored, enable governments to construct detailed profiles of their citizens, and increase the risk of personal information falling into the wrong hands. Authorities could also

---

[21] Foundation for Media Alternatives and Privacy International. (2016). Stakeholder Report Universal Periodic 27th Session: The Right to Privacy in the Philippines. https://www.fma.ph/wp-content/uploads/2017/07/UPR27_philippines_0.pdf

[22] Rappler. (2022, January 13). Comelec data leaked by hackers. *RAPPLER*. https://www.rappler.com/nation/elections/127315-comelec-data-hackers/

[23] Fowler, J. (2023, April 18). Philippines Police Employee Records Leaked Online in a Massive Data Breach. *vpnMentor*. https://www.vpnmentor.com/news/report-philippine-police-breach/

selectively restrict, censor or block internet connections for specific individuals or groups, leading to harassment and persecution. In the case of data breaches, the government has no remedy or compensation for the victim parties, and for larger corporations and organizations, the government is not ready to shoulder such large damage.

D. Additional means of unlawful data usage

In recent news, the National Telecommunications Commission (NTC) in the Philippines has permitted telecommunication companies to use the data gathered from SIM card registration for marketing purposes. While this decision has raised concerns about consumer privacy and data protection, it also highlights the broader issue of how SIM card registration can enable authorities to easily monitor an individual's activities, movements, and interests. As a SIM card is more than just a phone number, the potential misuse of this data can have serious implications for personal privacy and surveillance. In this context, it is important to consider the balance between the need for law enforcement and the protection of individual privacy rights.

For Marketing Purposes

Telecommunications companies in the Philippines are considering the use of data obtained from SIM card registration for marketing purposes. The misuse of user data for commercial and political purposes, as telecommunication companies have expressed their interest in using the data for marketing purposes. It is important to strike a balance between privacy and security concerns and ensure that any measure taken does not unreasonably infringe on fundamental rights.

This practice may raise concerns about data privacy and the use of personal information. The Data Privacy Act of 2012 mandates that personal information obtained by companies should be used only for the purpose it was collected, and obtaining consent from customers is crucial. The National Privacy Commission has emphasized the need for companies to be transparent about their data collection and processing practices to ensure that they comply with data privacy laws. Telecommunications companies must ensure that the use of customer data for marketing purposes is lawful, ethical, and transparent to protect customers' privacy rights.

The Philippines' National Telecommunications Commission (NTC) recently allowed PTEs to use the data obtained from SIM card registration for **marketing purposes**[24]. This decision has raised concerns among consumers, particularly regarding their privacy. While telcos claim that the data will only be used to improve their services, critics argue that this move could potentially lead to unwanted marketing and spam messages. The NTC assures that the use of the data will be strictly regulated and will require customers' consent. However, given the history of data privacy breaches in the country, many are skeptical about the effectiveness of these regulations. Moreover, the NTC has yet to **clarify the exact details of how the data will be used**, causing further alarm among privacy

[24] Yu, L. S. (2023, March 7). Watch what you consent to: Telcos may use SIM registration data for marketing. *RAPPLER*. https://www.rappler.com/business/telecommunication-companies-may-use-data-sim-registration-marketing-purposes/

advocates. Overall, while telcos hope to benefit from this new marketing strategy, they need to tread carefully and prioritize their customers' privacy to avoid backlash and potential legal consequences.

It has also drawn opposition from various groups due to the potential threats it poses to privacy and free speech. Privacy is a fundamental human right recognized by many international instruments and national laws. Anonymity is also crucial to protect the privacy of whistleblowers, journalists, human rights defenders, and members of the opposition. SIM card registration can undermine this anonymity and put vulnerable groups at risk of surveillance, harassment, and discrimination. Additionally, the registration system can be costly, inefficient, and prone to errors, making it unlikely to effectively deter criminal activities.

For Monitoring Purposes

A SIM card is more than a phone number. It allows authorities to easily track people's locations and movements. All of their online activity—websites visited, search queries, purchases, and more—can be traced back to their device[25]. By tracking the location of a SIM card, authorities can easily determine an individual's movements and whereabouts, potentially invading their privacy and exposing them to surveillance. This data can also be used to create a detailed profile of the individual's daily routines, activities, and interests.

Under Section 10 of the RA. No. 11934, Public Telecommunications Entities (PTEs) are to provide information obtained during the registration process upon the issuance of a subpoena by competent authorities, but only in cases where a specific mobile number is being used in the commission of a crime or as a means to commit malicious, fraudulent, or unlawful acts.

While the provision intends to combat crime and protect the public, it could potentially be abused by the authorities. The provision allowing the authorities to access information only upon the issuance of a subpoena by a competent authority may be circumvented, and the authorities could use the data for other purposes.

For instance, authorities could use this provision to track down and monitor individuals critical of the government or other dissidents under the pretext of investigating a crime. This can have serious implications for their personal safety and freedom of expression, as well as their ability to participate in democratic processes and hold their government accountable. This could result in the violation of the privacy and freedom of speech of these individuals, as the authorities could use the data to harass or intimidate them.

Furthermore, it can have a broader chilling effect on freedom of expression and assembly, as individuals may self-censor out of fear of being monitored or

[25] Bischoff, P., & 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/

targeted by the government. This undermines the democratic principles of transparency, accountability, and free speech that are essential for the functioning of a healthy democracy.

In addition, the provision does not require the authorities to notify the affected individuals when their data is being accessed, leaving them in the dark about potential privacy violations. This lack of transparency could be exploited by the authorities to conduct secret surveillance and infringe on the privacy rights of individuals.

Overall, while the provision is intended to combat crime, it is essential to ensure that it is not abused by the authorities to infringe on the privacy and freedom of speech of individuals. Stricter oversight and transparency measures are necessary to ensure that the provision is used for its intended purpose and does not lead to the violation of fundamental rights.

Risk of Identity Theft

Identity theft on SIM replacement is a potential risk associated with mandatory SIM card registration. In some cases, individuals may need to replace their SIM cards due to loss, damage, or theft. To obtain a replacement SIM card, registered mobile users are required to present a valid ID and an affidavit of loss of their SIM card to their telecom provider, as stated by DICT spokesperson and Undersecretary Anna Mae Lamentillo.[26]

However, this process can be exploited by cyber-thieves through a technique called SIM swapping. Attackers can use this technique to obtain replacement SIM cards that do not belong to them from a telecom operator and use the victim's mobile number for fraudulent activities. To carry out this attack, the attacker must have access to important personal information about the victim, which can be obtained through various means such as searching the web for publicly available information or social engineering.[27]

Once the attacker has control of the victim's phone number, they can exploit mobile authentication as a backdoor for fraudulent transactions. This can give the attacker access to the victim's sensitive information, including bank account details, social media accounts, and email accounts. In the words of Privacy Commissioner and Chairman Raymund Enriquez Liboro, "A SIM card in the hands of a cyber thief makes mobile authentication meaningless, as it becomes almost like a master key for committing all sorts of identity fraud. It leaves the victim’s

[26] Cruz, R. C. D. (2023, January 19). *Stolen, lost registered SIM cards can be remade: Dict*. Philippine News Agency. https://www.pna.gov.ph/articles/1193119
[27] Imi. (2022, March 11). *SIM card swapping and cell phone hijacking - device identity theft*. Identity Management Institute®. https://identitymanagementinstitute.org/sim-card-swapping-and-cell-phone-hijacking/

personal data vulnerable to all sorts of misuse and abuse, including access to email and Facebook accounts, and unauthorized ATM and online bank withdrawals."[28]

In the case of Eric Meiggs and Declan Harrington[29], it demonstrates the serious harm that identity theft can cause. These two individuals were sentenced for their involvement in an extensive scheme to take over victims' social media accounts and steal their cryptocurrency with the use of SIM swapping and other techniques which allowed them to bypass security measures and gain access to sensitive information. The victims of Meiggs and Harrington suffered significant financial losses, and their personal information was compromised.

[28] *NPC makes telco take measures against sim-swap fraud; public warned on identity theft*. National Privacy Commission. (2021, November 11). https://www.privacy.gov.ph/2018/01/npc-makes-telco-take-measures-against-sim-swap-fraud-public-warned-on-identity-theft/

[29] *Two men sentenced for nationwide scheme to steal social media accounts and cryptocurrency*. The United States Department of Justice. (2022, October 19). https://www.justice.gov/opa/pr/two-men-sentenced-nationwide-scheme-steal-social-media-accounts-and-cryptocurrency

E. Other threats and dangers to registered SIM card holders

The mandatory SIM registration does not even solve the problem as Scammers use VOIP messaging services overseas and not SIM cards. It uses the internet to send texts and/or calls to different carriers. They do not use SIMs[30]. For example, a scammer in Davao can use a VoIP service in Spain, routed via VPN in Switzerland to send a scam text to 1000 Globe/Smart subscribers in the Philippines. They could even use a program to list all possible numbers of some carriers.

Data privacy and protection is a matter of national security

As per privacy notice of Smart Telecommunication, published on the 25th of April 2023, have contracted ZOLOZ Global, an automated biometrics, identity detection and behavioral analytics company based in China. The notice states "Any Personal Data processed using the technology of ZOLOZ will be transmitted to the SIM Register of SMART immediately and will only be retained in ZOLOZ's systems for a maximum of three (3) months, solely for quality assurance and audit purposes. After which, ZOLOZ will securely and permanently destroy all Personal Data that it has processed on our behalf." However, in less than a day of this notice being posted it changed its policy to 1 day instead of 3 months, and now the page was removed from the site.

But if this were to be pushed through this means that ZOLOZ will delete the data on SMART's behalf . However ZOLOZ, which is a Chinese company, beholden to the CCP can be subjected to compliance under Chinese law to submit information under the interest of national security stated in Article 28 of the Cyber Security Law of the People's Republic of China, which states that *"Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."*[31] This compels network operators, which could be interpreted as social media platforms, application creators, and technology companies, such as ZOLOS, to hand over information when requested. Whatever data is processed by Zoloz can be transferred to servers in China, if judged necessary by the company or government.

In case of nationwide data breaches, what provisions of the law could be applied to mitigate and recover from such devastating consequences? What specific course of action shall the government do?

[30] Weber, J. (2019, January 31). Scammers and VoIP: What you need to know about illegal phone scams. VoipReview. https://www.voipreview.org/blog/scammers-and-voip-what-you-need-know-about-illegal-phone-scams

[31] 朱英. (n.d.). 中华人民共和国网络安全法_滚动新闻_中国政府网. http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

It is a fact that data breaches are unavoidable. The question now lies in how to deter its commission and combat the effects in case it happens. As stated in the SIM Registration Act, the penalty for breach of confidentiality or breach of confidentiality due to negligence is a fine of Five hundred thousand pesos (P500,000.00) up to Four million pesos (P4,000,000.00). In case of cyber-attacks, the incident is to be reported to the Department of Information and Communications Technology within 24 hours of detection[32]. Although the penalties and course of action of PTCs are outlined, it does not clearly state the specific course of action that the DICT should do.

How competent is the government in providing protection to its citizens in terms of securing their privacy?

As per the law, a court order is necessary in order to access information held by the telecommunications company. That is true however this shows how our lawmakers are ignorant about tech. The requirement of a court order is a remnant of the wiretapping law. Because it would not be the law enforcers who would be the ones to manually tap the target's landline but it will be the phone company who taps in recorders and other listening devices to junction box terminals so they also need extended networks. Wireless communication surveillance can be done by the agent themselves, remotely and covertly without the help of outsiders. Even employees in the NSA abuse their position and make use of their numerous surveillance apparatus for personal uses such as spying on their spouses[33]. How can we trust our government officials and state officers to not do the same?

Infectivity and poor implementation of SIM registration

Mexico authorized the use of biometrics registration for mobile phones. The cellphone registration, otherwise known as Registro Nacional de Usuarios de Telefonía Móvil or RENAUT, was the first nationwide implementation, which aimed to prevent mobile-aided crimes. It requires the name, national ID, telephone number, SIM card activation date, social security number, and biometric data. Enforced in 2010, however, the kidnapping rate in the country rose to its highest since 1971. Thus the law was abolished in 2012[34]. How do we know that the Philippines won't face a similar outcome? How can we guarantee that this law will be implemented properly?

Malaysia began their SIM card registration in 2006 which *"Aim to restrain misuse of public mobile communications services and secure national security against terrorism and criminal activities."* However, even in 2019, more than 15 years after its implementation, six telecom companies have registered prepaid SIM cards, without further verification. Similar cases also arose in 2020.

---

[32] SIM Registration Act of 2022, Rep. Act No. 11934, § 11(b)(c), (July 25, 2022) (Phil.).
[33] Selyukh, A. (2013, September 27). NSA staff used spy tools on spouses, ex-lovers: watchdog. U.S. https://www.reuters.com/article/us-usa-surveillance-watchdog-idUSBRE98Q14G20130927
[34] De Guzman, J. (2022, June 9). SIM card registration: How other countries do it. RAPPLER. https://www.rappler.com/newsbreak/iq/how-other-countries-implement-sim-card-registration/

CONCLUSION

For the reasons set forth above, the team respectfully submits that Republic Act No. 11934, otherwise known as the Subscriber Identity Module (SIM) Registration Act, and National Telecommunications Commission Memorandum Circular No. 001-12-2022, or the Rules and Regulations Implementing Republic Act No. 11934, are unconstitutional for being violative of the right to privacy under Section 3(1), Article III of the 1987 Constitution, and are inconsistent with the provisions of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012.

Although the said law has noble ends of protecting the citizens from being victims of malicious use of technology, its means of implementing so are contrary to the Data Privacy Act's provisions and also breaching the Filipinos' constitutional right to privacy.

It is clear that although there are portions of the law that justifies the protection of the data transmitted by SIM card holders during their registration, it clearly does not guarantee the protection of the end users' data as they no longer have control over the information they have shared. The penalties imposed in R.A. 11934 do not justify the damages and loss in the occurrence of an act that discloses a massive amount of information pertaining to the users. Furthermore, the mere fact that the subscribers are forced to disclose their personal information to the state already violates their constitutional right to privacy since refusing to do so inhibits their ability to enjoy their freedom of expression as well as to make necessary daily conversations through the use of mobile network services.

It is true that privacy and security are not completely contradictory concepts. In fact, they are mutually reinforcing values that both need to be upheld for the benefit of the people. That said, privacy is a human right, and as such, it should not be sacrificed so easily. Surrendering it, together with access to communication, in favor of a token level of security is a bargain that Filipinos should not be taking in compliance with the R.A. 10173 as well as own very own 1987 Philippine Constitution, which the current R.A. 11934 is not consistent and compatible with.