A MEMORANDUM NEGATING 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:

Jay Paanud Tejada - Head Researcher
Lord Christian Regacho - Closing Statement
Ivan Ric Woogue - Head Researcher
Jose Glen Samson - Assistant Researcher
Erik Miguel Celdran - Assistant Researcher
Denzel John Lawas - Assistant Researcher
Christian Anthony Stewart - Head Researcher
Reigina Yshanni Mascariñas - Assistant Researcher
Ralph Byron Boter - Assistant Researcher
Jastine Ouano Guzman - Rebuttalist
John Daves Baguio - Oralist
John Anthony Torrejas - Assistant Researcher
Vladimir Roman - Assistant Researcher

May 3, 2023

TABLE OF CONTENTS

INDEX OF AUTHORITIES

Philippine Laws

Philippine Jurisprudence

US Jurisprudence

Books, Articles, and Journals

https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it..... 2

Rosales, E. F. (2022, October 4). Pinoys lost millions of dollars to text scams – government. Philstar.com. https://www.philstar.com/headlines/2022/10/05/2214382/pinoys-lost-millions-dollars-text-scams-government..... 3

Baclig, C. E. (2022, June 24). PH biggest target of phishing in Southeast Asia—cybersecurity report | Inquirer News. INQUIRER.net. https://newsinfo.inquirer.net/1615655/for-posting-edited-ph-biggest-target-of-phishing-in-southeast-asia-cybersecurity-report..... 3

Hilotin, J., & Bloomberg, W. I. F. (2022, September 7). Philippine text scams: Customer names 'harvested', SMS with receivers' names trigger probes. Gulf News. https://gulfnews.com/business/philippine-text-scams-customer-names-harvested-sms-with-receivers-names-trigger-probes-1.1662515019484..... 3

TeleGeography. (2016, July 25). Poland launches pre-paid SIM registration. CommsUpdate. https://www.commsupdate.com/articles/2016/07/25/poland-launches-pre-paid-sim-registration/..... 8

Timeline of SIM Card Registration Laws. (2022, May 16). Privacy International. https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws.....8

TeleGeography. (2016a, May 17). Belgium to implement pre-paid SIM registration this year. CommsUpdate. https://www.commsupdate.com/articles/2016/05/17/belgium-to-implement-pre-paid-sim-registration-this-year//..... 8

West Yorkshire Police. (n.d.). *The 10 Principles of Crime Prevention | West Yorkshire Police*. https://www.westyorkshire.police.uk/advice/10-principles-crime-prevention/10-principles-crime-prevention/10-principles-crime-prevention..... 13

Yongo, E., Lowe, C., & Theodorou, Y. (2021). Access to Mobile Services and Proof of Identity 2021. Groupe Speciale Mobile Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf?fbclid=IwAR3aW24HIb_BuEu0AqbDl4tzYYZy3odweCyhv1szTlDZ1sfAh_-ATB4BzZA..... xi, 13, 15

Proposed Mandatory Registration of Subscriber Identity Modules (SIMs) used for Publicly Available Electronic Communications Services Regulations. (2018, August). Malta Communications Authority. https://www.mca.org.mt/sites/default/files/Public%20Consultation%20DOCUMENT%20-%20SIMs.pdf..... 13, 16

Theodorou, Y., Okong'o, K., & Yongo, E. (2019). Access to Mobile Services and Proof of Identity 2019. Groupe Speciale Mobile Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf..... 13, 16

Sheng, Y. (2021, February 19). Real-name registration for prepaid SIM cards will help prevent crimes. Chinadailyhk. https://www.chinadailyhk.com/article/158085#Real-name-registration-for-prepaid-SIM-cards-will-help-prevent-crimes..... 15

Real-name Registration Programme for Subscriber Identification Module (SIM) Cards. (2023, April 27). Office of the Communications Authority. https://www.ofca.gov.hk/en/consumer_focus/guide/hot_topics/sim_registration/index.html..... 15

Piad, J. M. A., Tyrone Jasper C. (2022, September 7). Salceda suspects contact tracing as source of data leak. INQUIRER.net. https://newsinfo.inquirer.net/1659610/salceda-suspects-contact-tracing-as-source-of-data-leak.....17

FOREWORD

This section shall serve as an introduction to and explanation of the legal issue presented and laws involved.

Republic Act No. 11934 or more commonly known as the Subscriber Identity Module (SIM) Registration Act[1], requires all users of prepaid SIM cards to register their personal information with their respective telecommunications companies, ostensibly to address issues related to national security and criminality. The Rules and Regulations on implementing the SIM Registration Act can be viewed within the National Telecommunications Commission Memorandum Circular No. 001-12-2022[2]. The National Telecommunications Commission or NTC is primarily responsible for the regulation and quasi-judicial functions relative to the supervision, adjudication, and control of the country's telecommunications, telecommunications, and broadcast, including cable television facilities and services.

In the National Telecommunications Commission Memorandum Circular No. 001-12-2022, the following rules and regulations to be adhered at all times upon its implementation:

SIM Registration

- All end users including foreigners are required to register their SIMs, embedded SIMs(eSIMs) and other variations to their respective telecommunication providers.
- Failure to comply with the requirements as stated in Section 6 of the National Telecommunications Commission Memorandum Circular No. 001-12-2022[2] would result in their SIM to not be activated.
- Registration must be free of charge.

Registration of Existing Subscribers

- Existing Subscribers have one hundred eighty (180) days to comply for the registration of their SIMs upon the effectivity of the Act.
- The registration period for existing subscribers may be extended for at most one hundred twenty (120) days.
- Failure to comply for the registration will result the deactivation of their SIMs

Registration Form and Registration Process

- The registration process must be completed electronically provided by their respective telecommunication providers.
- The following requirements must be complied in accordance with type of end user:

  By individual (natural person) end-user;

  1. Full Name
  2. Date of Birth

[1] Subscriber Identity Module (SIM) Card Registration Act, Rep. Act No. 11934, (Sept. 19, 2022) (Phil.), https://www.officialgazette.gov.ph/2022/10/10/republic-act-no-11934/

[2] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

3. Sex
4. Address
5. Identity Document (ID)
6. ID Number

By juridical entity end-user;

1. Business Name
2. Business Address
3. Full Name of Authorized Signatory

By foreign national end-user;

1. Full Name
2. Nationality
3. Date of Birth
4. Passport
5. Address in the Philippines
6. For Persons of Concern or POCs, the Type of Travel or Admission Document Presented
7. ID Number or Number of Document Presented

There have been concerns raised by various groups and individuals that these laws are unconstitutional and violate the right to privacy enshrined in the Philippine Constitution. Section 3(1), Article III of the 1987 Constitution[3] explicitly provides 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.".

Critics argue that the SIM registration laws go beyond what is allowed by the Constitution, as they require the disclosure of personal information, including the user's full name, address, date of birth, and government-issued ID number. They also argue that the laws are inconsistent with the provisions of Republic Act No. 10173, or the Data Privacy Act of 2012[4], which requires the protection of personal information and the respect of privacy rights. The Implementing Rules and Regulations of the DPA[5] expressively lays down in detail the grounds for collecting and safeguarding data, rights of the data subject, fines and punishment for those negligent to the confidentiality of data, and many more.

Here are the key points of the Implementing Rules and Regulations of Republic Act. No. 10173[5]:

- Personal Data controllers and processors must process data in a lawful, fair, and transparent manner.
- Individuals have the right to access and correct their personal data, as well as to object to its processing and erasure.
- Personal data can only be transferred to third parties in certain circumstances such as when the individual has given consent or when there is legal obligation to do so.

[3] Const., (1987), art. III (Phil.)
[4] Data Privacy Act of 2012, Rep. Act No. 10173, (Aug. 15 2012) (Phil.), https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/
[5] Implementing Rules and Regulations of the Data Privacy Act of 2012, Department of Information and Communications Technology, 13 September 2016.

- Personal data breaches must be reported to the National Privacy Commission (NPC), and affected individuals must be notified as soon as possible.
- The NPC has the power to investigate and impose penalties for violations of the Data Privacy Act, including fines and imprisonment.
- Organizations must implement appropriate security measures to protect personal data from unauthorized access, use, or disclosure.
- Organizations must appoint a data protection officer (DPO) to oversee their data protection practices.
- Organizations must conduct privacy impact assessments (PIAs) before implementing new data processing activities that may pose a high risk to individual's privacy rights.
- Organizations must comply with other requirements, such as providing privacy notices to individuals, obtaining consent for certain types of data processing, and ensuring the accuracy of personal data.
- Individuals have the right to file complaints with the NPC if they believe that their privacy data rights have been violated.

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

For us to negate the unconstitutionality of Republic Act No. 11934, otherwise known as the Subscriber Identity Module (SIM) Registration Act[6], and National Telecommunications Commission Memorandum Circular No. 001-12-2022[7], or the rules and regulations implementing republic act no. 11934, we need to know and address the issues presented.

In the Philippines, all users of prepaid mobile phone services are required to register their SIM cards by this legislation with their personal information. This designed registration procedure is made to stop unregistered SIM cards from being used in any criminal activities such as terrorism, kidnapping, and extortion.

Republic Act No. 11934, otherwise known as the Subscriber Identity Module (SIM) Registration Act is a legislation enacted in the Philippines that requires the individuals who use prepaid mobile phone services to register their SIM cards with their personal information. The process of registration is not out of the ordinary for other account creation that requires personal information such as name, date of birth, address, type of identification, and ID number. There are several advantages that this act provides, such as making the SIM card identifiable with its owner's information, it targets scammer's activities that will eventually lead to reducing scams. Scams and other illegal activity related to it increases each year in the Philippines, and the Republic Act No. 11934 or SIM Registration Act helps the authorities in tracking and stopping the criminal act. With the continuous rise of digital communication, digital crimes also increase along with it. This act is essential to promote the common good and safety of the general public.

The Republic Act No. 11934 or SIM Registration Act complies with the Implementing Rules and Regulations of Data Privacy Act of 2012[8] by providing privacy notice to the subscribers to inform them of the processing of their personal information and enabling them to exercise their rights as data subjects. Confidentiality clause is also included to prohibit the disclosure of personal information obtained during the SIM registration, except for any specific circumstances outlined in the law or has a probable cause. This ensures that the privacy rights of the users are protected and is used to combate criminal activities

In 1996, President Fidel V. Ramos[9] signed Administrative Order (AO) 308, which aimed to create a decentralized national computerized identification system for government agencies, but it was invalidated by the Supreme Court due to its vagueness and lack of safeguards for privacy. On the other hand, in 2005, President Gloria Arroyo signed Executive Order (EO) 420, establishing the Unified Multi-Purpose Identification (UMID) System, which was upheld by the Supreme Court in the Kilusang Mayo Uno (KMU) case due to its specificity and privacy safeguards.[10] The court cited the Whalen vs Roe[11] case, which upheld a New York law requiring physicians to disclose private health information to the state to control the distribution of dangerous drugs, to support the constitutionality of EO 420. Similarly, the SIM Registration Act could be argued to be constitutional based on its specific enumeration of data required and safeguards, and the fact that the data are already held by existing government ID systems.

---

[6] Subscriber Identity Module (SIM) Card Registration Act, Rep. Act No. 11934, (Sept. 19, 2022) (Phil.), https://www.officialgazette.gov.ph/2022/10/10/republic-act-no-11934/

[7] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

[8] Data Privacy Act of 2012, Rep. Act No. 10173, (Aug. 15 2012) (Phil.), https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/

[9] Ople v. Torres, G.R. No. 127865 (July 23, 1998) (Phil.)

[10] Kilusang Mayo Uno v. Director General, National Economic Development Authority, G.R. No. 167798 (Apr. 19, 2006) (Phil.)

[11] Whalen v. Roe, 429 U.S. 589 (1977)

Mandatory SIM card registration is a policy that requires mobile network operators to collect and verify the identification and personal information of individuals before activating a prepaid mobile SIM card in their name. This policy is aimed at enhancing security and preventing the use of mobile services for criminal activities. As of February 2021, 157 countries have implemented this policy.[12] The reasons for implementing this policy may vary depending on the country, but it is often seen as an effective way to prevent the misuse of mobile services and ensure that mobile networks are used for legitimate purposes. Some examples of countries that have implemented this policy include Austria, Indonesia, Poland, and Belgium. Critics have expressed concerns about the impact of this policy on privacy and freedom of expression.

[12] Yongo, E., Lowe, C., & Theodorou, Y. (2021). Access to Mobile Services and Proof of Identity 2021. Groupe Speciale Mobile Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf?fbclid=IwAR3aW24HIb_BuEu0AqbDl4tzYYZy3odweCyhv1szTlDZ1sfAh_-ATB4BzZA

ARGUMENTS

In this section, the negative side will discuss the arguments gathered strenuously from their research on why the R.A. (Republic Act) 11934 or Subscriber Identity Module (SIM) Registration Act and National Telecommunications Commission (NTC) Memorandum Circular No. 001-12-2022 are not unconstitutional and are consistent and compatible with R.A. 10173 or Data Privacy Act of 2012 and its Implementing Rules and Regulations (IRR). In the interest of writability for the negative side and readability for the readers, the term SIM Registration Act shall be utilized instead of the official legislative reference R.A. 11934. And, the NTC Memorandum will be used instead of NTC Memorandum Circular No. 001-12-2022. Similarly, the Data Privacy Act (DPA) shall be employed in place of the statutory reference R.A. 10173. By doing so, the goal is to achieve greater concision and readability in this memorandum, while simultaneously ensuring that the relevant legislation is accurately represented and upheld.

Purpose of the SIM Registration Act

The negative side would like to begin by stating the purpose of the creation of the SIM Registration Act. In Section 2 of the SIM Registration Act[13], it is stated "... The introduction of modern telecommunications technology with the view of providing the widest information dissemination is greatly encouraged. The possession of the most modern technology carries with it tremendous responsibility. Towards this end, a mechanism for the effective use of technology for the common good and not any illegal or malicious purpose must be established." The stated section can be broken down in 3 parts:

- Wide dissemination of information made available by technology
- Responsibility of such capability
- Statute ensuring it is not used for malicious purposes

Undoubtedly, the ever-evolving landscape of technology has facilitated the dissemination of information at an unprecedented scale and speed utilizing simplistic methods such as online postings or social media interactions. A SIM is part of this technology where it is a plastic piece with a circuit-embedded chip that stores identifying information on a mobile device.[14] The SIM's pivotal role in telecommunications lies in its ability to establish a linkage between a physical device and its proprietor, thereby enabling efficient routing of calls to the appropriate user device.[1] In 2022, the number of mobile subscribers in the Philippines is around 153 million.[15] With this amount of people, a logical inference can be made that dissemination of information through Short Message Service (SMS) text messages can reach a massive audience with the caveat that the recipient's phone number must be known.

Individuals possessing the capability to disseminate information on a wide scale bear a weighty responsibility to utilize this capability in a manner that is not detrimental to the peace and order of society. The potential consequences of irresponsible or malicious conduct with respect to the dissemination of information can be severe and can range from the dissemination of false information on certain domains such as politics, health, and the economy to the propagation of dangerous or unsettling pranks such as the dissemination of false alarms like invasion attacks or bomb threats. Sadly, one of the most common forms of misuse of short message service (SMS) text messaging is the practice of "smishing" which is the mobile text

[13] Subscriber Identity Module (SIM) Card Registration Act, Rep. Act No. 11934, (Sept. 19, 2022) (Phil.), https://www.officialgazette.gov.ph/2022/10/10/republic-act-no-11934/

[14] Xu, T. (2021, March 30). What Is a SIM Card and How Does It Work? Built In. https://builtin.com/hardware/what-is-a-sim-card

[15] Statista Research Department. (2023, April 28). Philippine: mobile subscribers count 2022. Statista. https://www.statista.com/statistics/1010926/total-number-mobile-subscribers-philippines/#:~:text=Total%20number%20of%20mobile%20subscribers%20Philippines%202012%2D2022&text=In%202022%2C%20the%20number%20of,comparison%20to%20the%20previous%20year.

messaging version of a phishing cybersecurity attack. Its method employs the dissemination of a text message containing a malicious link, with the objective of luring the recipient into clicking on it, thereby resulting in the theft of their personal data through either the downloading of malware or the surreptitious acquisition of their login credentials.[16]

The rapid and widespread dissemination of information enabled by technology, such as through the use of SMS text messaging, has given individuals an unprecedented level of power to convey their messages efficiently and effectively. However, with this kind of capability also comes an inherent danger as malicious actors can exploit these capabilities to target a wider audience for the purposes of scamming or phishing unsuspecting victims. In order to ensure that the state is able to strike an appropriate balance between protecting its citizens from such abuses, while also respecting and upholding their privacy, the SIM Registration Act was enacted with the sole purpose of preventing the malicious use of such technologies.

Advantages of the SIM Registration Act

The benefits from the enactment of this legislation will be dived deep in detail within this section. Through this discussion, the readers will be more informed on the positive outcomes that can arise from the enactment of this law and its positive impact on society. Through an open-minded perspective surrounding this legislation, readers can understand the motives behind its implementation and its potential to promote the common good and safety of the general public. By examining the implications of this law without bias, individuals can more effectively evaluate the efficacy and relevance of this legislation to contemporary society.

Identifiable SIM Owner

In Section 4 (3) of the NTC Memorandum[17], it states "All the SIMs to be sold and/or issued by the Public Telecommunications Entities (PTEs), its agents resellers, or any entity shall be in a deactivated state… It shall only be activated state as defined after the end-user completes the process of registration." Some terms need to be defined first before proceeding to the rest of the discussion. A PTE is any person, natural or judicial, government or private, engaged in the provision of telecommunications services to the public for compensation, as defined under Republic Act No. 7925, as amended, or the Public Telecommunications Policy Act of the Philippines. A SIM card in a deactivated state means that it is incapable of being used for outgoing and incoming calls, internet access, sending, and receiving messages. On the other hand, a SIM card in an activated state is just the opposite of a SIM card in a deactivated state.

This section basically means that people planning to buy new SIM cards for purposes of using a dummy phone number for spamming SMS text messages will have a difficult time since they have to give their personal details for the new SIM card to be in activated state. In Section 6 (4) of the NTC Memorandum[8], it states the following personal information and other information needed for the registration. For the natural person, 6 information is required: (1) full name, (2) date of birth, (3) sex, (4) present/official address depending on the end-user, (5) type of identification (ID) presented, and (6) ID number presented. For the juridical entity, 3 information is required: (1) business name, (2) business address, (3) full name of authorized signatory. Lastly for a foreign national end-user, 7 information is required: (1) full name, (2) nationality, (3) date of birth, (4) passport, (5) address in Philippines, (6) for persons of

[16] Kaspersky. (2023, April 19). What is Smishing and How to Defend Against it. https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[17] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

concern (POCs), the type of travel or admission document presented, and (7) ID number or number of document presented. Lastly for the 3 mentioned above, they have to secure a (1) photo of the valid government-issued identification (ID) card or other similar form of document and input (2) the assigned mobile number of the SIM with its serial number.

There is nothing out of the ordinary of the required information for the SIM registration. In fact, these are commonly asked for personal information when creating social media accounts, banking accounts, delivery accounts like Amazon or Lazada or even getting a government ID such as a driver's license. The most sensitive information here is the personal government-issued ID for natural persons, passport for foreigners, and business name and full name of authorized person for juridical entities. The reason why these are considered as sensitive information is because these can actually point to a person, so the owner of the new SIM can actually be traced back to a person due to these sensitive information.

Targets Scammers and Lessens Scams

Scams have become a prevalent issue in today's society, with countless individuals falling victim to them each year. With new technology and the rise of digital communication, new opportunities are created for scammers, who can now target individuals through text messages, emails, and social media. In the Philippines, the problem has reached alarming levels, with millions of dollars lost to text scams alone.

A recent example of the Philippines' text scam problem was highlighted in a Gulf News[18] article, which revealed that fraudsters are harvesting customer names through text messages. These scams involve sending SMS messages to individuals, which appear to be from a legitimate company or organization. The messages typically ask for personal information, such as names, addresses, and contact details. In some cases, the scammers use the victim's name in the message, creating a false sense of legitimacy. This tactic has triggered investigations, and authorities are now cracking down on these types of scams.

The Philippines' government has also been trying to tackle the issue of scams. According to a report in the Philippine Star[19], the government has been working to crack down on text scams and other forms of fraud. Unfortunately, despite these efforts, millions of dollars are still lost each year due to scams. This indicates that there is still much work to be done in terms of educating the public and taking decisive action against fraudsters.

Another type of scam that is becoming increasingly common in the Philippines is phishing. In a report by the Inquirer, it was revealed that the Philippines is the biggest target of phishing attacks in Southeast Asia. Phishing scams involve fraudsters sending fake emails or messages, which appear to be from a legitimate source, in order to obtain sensitive information such as passwords and credit card numbers[20]. These types of scams are particularly dangerous because they can lead to identity theft and financial loss.

---

[18] Hilotin, J., & Bloomberg, W. I. F. (2022, September 7). Philippine text scams: Customer names 'harvested', SMS with receivers' names trigger probes. Gulf News. https://gulfnews.com/business/philippine-text-scams-customer-names-harvested-sms-with-receivers-names-trigger-probes-1.1662515019484

[19] Rosales, E. F. (2022, October 4). Pinoys lost millions of dollars to text scams – government. Philstar.com. https://www.philstar.com/headlines/2022/10/05/2214382/pinoys-lost-millions-dollars-text-scams-government

[20] Baclig, C. E. (2022, June 24). PH biggest target of phishing in Southeast Asia—cybersecurity report | Inquirer News. INQUIRER.net. https://newsinfo.inquirer.net/1615655/for-posting-edited-ph-biggest-target-of-phishing-in-southeast-asia-cybersecurity-report

The issue of scams is a complex and multifaceted problem that requires a concerted effort from both the public and private sectors. Individuals must be vigilant and cautious when sharing personal information or responding to unsolicited messages. Meanwhile, companies and organizations must take steps to protect their customers from scams and cyber threats. Governments must also play a role in regulating and monitoring fraudulent activities, as well as educating the public about how to avoid scams.

Evidently, scams have become a pervasive problem in the Philippines, with text scams, phishing scams, and other types of fraud causing millions of dollars in losses each year. While efforts are being made to crack down on these types of scams, more needs to be done to raise awareness and protect individuals from falling victim to fraudsters. It appears that much is still required to reduce the impact of scams and ensure a safer digital environment for all.

People who spam fraudulent text messages to a wide range of people are the first to be negatively affected by the SIM Registration Act. It will be very difficult for them to set up a new fake person for every new SIM card. If they do use their own personal information to register a SIM card, their activity can be easily traced back to them. If they started sending fraudulent, fake advertisements, scams, and other nefarious SMS text messages, they can be reported and be caught by the authorities.

If a user receives a fraudulent text message or call, the user can report them to their respective PTE. And, the PTE is obligated to provide a user-friendly reporting mechanism to report any potentially fraudulent SMS activity under Section 10 (11) of the NTC Memorandum[9]. Upon due investigation, the PTE is obligated to deactivate, temporarily or permanently, the SIM used for fraudulent SMS activity until further notice under Section 10 (7) of the NTC Memorandum[21]. This easily prevents the scammer from imposing more damage using the SIM as the authorities will look for them.

Scammers often utilize fraudulent or fake personal information when registering a SIM card, which is a highly viable strategy for their illegal activities. Nevertheless, there are severe consequences for anyone found guilty of such acts. Section 13 of NTC Memorandum[9] stipulates that providing false or fictitious information or using fraudulent identification documents to register a SIM card can result in a prison term of 6 months to 2 years, a fine of not less than ₱100,000.00 but not more than ₱300,000.00, or both. Moreover, sellers of registered SIMs with personal identification information that does not match with the upcoming new owner can also face imprisonment ranging from 6 months to 6 years, in accordance with Section 14 of NTC Memorandum.[9]

Even the selling of stolen SIM cards is punishable under this statute. As mentioned in Section 17 of NTC Memorandum[9], any PTE, its agent, resellers, or entities engaged in the sale of stolen SIMs shall be held criminally liable. Those who engage in the sale of stolen SIMs will be subjected to a prison term of 6 months to 2 years, a fine not less than ₱100,000.00, or both. The law also includes provisions that penalize individuals who provide scammers with activated SIM cards or aid and abet in the commission of any offenses listed in the Act. Such individuals can be punished as co-principals and are also susceptible to penalties under the Revised Penal Code, as discussed in Section 20 of NTC Memorandum[9].

Due to the stringent penalties outlined in the statute, a sense of fear will be created among those who are contemplating to be scammers but doubting so much that they will

[21] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

opt to not go through. Thus, less spam messages will circulate through the SMS which means lesser chance of victims falling into the trap of phishing attacks.

The severe penalties outlined in the statute will create a sense of fear among those contemplating scams resulting in fewer spam messages circulating through SMS and a lesser chance of individuals falling prey to phishing attacks. Additionally, these penalties discourage bad actors from providing scammers with dummy activated SIM cards since doing so is punishable by this Act.

Helps Solve Cases

Similar with other activities or endeavors, communication plays a major role in the commission and execution of a crime especially when there are more than one participants which could be a principal, accomplice or an accessory. SMS text messaging is very valuable to these people because of the anonymity it provides compared to other mediums of communication like social media, for instance. If criminals used their personal Facebook to communicate with each other, they can still be easily identified by the authorities. A workaround they can employ is the creation of a new account. Without the SIM Registration Act, they can easily buy a new SIM card to be used as the new mobile phone number for the new account. Additionally if the criminal opts to use their SIM card number, it is impossible or highly unlikely to identify the owner of the SIM registration number. But if the SIM Registration Act was implemented, it will be easy to identify the owner of the SIM card and will make the creation of new accounts not a solid option due to the fact that the mobile number can be traced back to the identity of the owner.

In Nuez v. Cruz-Apao[22], the Supreme Court ruled that text messages are considered as valid evidence and can be used as such before court proceedings and even in administrative proceedings. In Rules on Electronic Evidence[23], Section 5 (k) of Rule 2 categorizes text messages as one of the examples of what is considered "Ephemeral electronic communication". And, Section 2 of Rule 11 is proving the parties of ephemeral electronic communications by the testimony of a person who was a party to the same or has personal knowledge thereof. If no witnesses can be produced, other competent evidence may be admitted. With the SIM Registration Act, there is no more competent evidence than the owner's identity of the SIM number.

In Section 10 of the SIM Registration Act[24] and in Section 12 of NTC Memorandum[9], PTEs shall be required to provide information obtained in the registration process only upon the issuance of a subpoena by a competent authority pursuant to an investigation based on a sworn written complaint that a specific mobile number, was utilized as a means to commit a malicious, fraudulent or unlawful act, and that the complaint is unable to ascertain the identity of the perpetrator. The SIM Registration Act complements the law Rules on Electronic Evidence by procuring the information used in the registration process of the SIM used as a means in the commission of an unlawful act or a crime. In cases whether civil or criminal, if the identity of the person of an SMS text message can be the key to solving a case or a dispute, it must be made available.

---

[22] Nuez v. Cruz-Apao, A.M. No. CA-05-18-P (Apr. 12, 2005) (Phil.)
[23] Rules on Electronic Evidence, A.M. No. 01-7-01-SC (July 17, 2001) (Phil.), https://www.set.gov.ph/resources/rules-on-electronic-evidence/#:~:text=Ephemeral%20electronic%20communication.,competent%20evidence%20may%20be%20admitted.
[24] Subscriber Identity Module (SIM) Card Registration Act, Rep. Act No. 11934, (Sept. 19, 2022) (Phil.), https://www.officialgazette.gov.ph/2022/10/10/republic-act-no-11934/

Deterrent to Future Crimes

For the discussion mentioned above, this Act can serve to deter future crimes. Difficulty in securing a dummy activated SIM card and the capability to produce the identity information of the SIM card owner within the provisions of the SIM Registration Act can make the commission of the crime harder by limiting the means of communication among the parties involved in the said crime. If a criminal objective is hard to accomplish, that difficulty will sow doubts on individuals hesitating to commit the crime that they will think twice and will be likely to decide not to pursue it in the end.

The West Yorkshire Police[25] provides general wisdom practiced by most people to deter crimes from happening to them. The 3rd principle or reducing the means is related to the removal of SMS messaging for communication of criminal activities. If there are less means to accomplish the crime, there will be less possible offenders due to some being not able to utilize the remaining means. Another principle is increasing the chances of being caught. An example of this principle is the use of surveillance cameras where people will think twice and hesitate before committing the crime since their movements and face can be captured by the camera and reviewed later on. The SIM Registration Act applies this as well where the identity of the SIM card thought to be involved in the commission of a crime can be revealed to the court.

In short, the SIM Registration Act can serve as an effective deterrent against the malicious use of SMS technology for illegal activities, thereby promoting the common good and safety of the general public.

Compliance with DPA and its IRR

Previously, the advantages of adopting the SIM Registration Act and the NTC Memorandum was thoroughly and comprehensively discussed. Nevertheless, it is crucial to note that the benefits of these statutes will be rendered meaningless if their provisions are not aligned with the regulations set forth by the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (IRR).

In this section of the Memorandum, the negative side will discuss how the SIM Registration Act and the NTC Memorandum are in compliance with the existing provisions set forth by the DPA and its IRR. It is of utmost importance that the SIM Registration Act and the NTC Memorandum are implemented in a manner that is consistent with the provisions of the DPA and its IRR to ensure that the public's privacy rights are protected.

Notice to Subscribers

The SIM Registration Act complies with the DPA in the integrity of protecting the privacy rights of its subscribers. [26]Section 16 of the DPA states that the data subject or the end-user has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. This is fulfilled through Section 6 (c) and Section 10 (c)[27] of the NTC Memorandum for the SIM Registration Act. Section 6 (c)

[25] West Yorkshire Police. (n.d.). The 10 Principles of Crime Prevention | West Yorkshire Police. https://www.westyorkshire.police.uk/advice/10-principles-crime-prevention/10-principles-crime-prevention/10-principles-crime-prevention

[26] Data Privacy Act of 2012, Rep. Act No. 10173, (Aug. 15 2012) (Phil.), https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/

[27] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the “Subscriber Identity Module (SIM) Registration Act”, Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

states that a privacy notice will be made available to the public via on their platform and website. The notice will explain the details in processing the personal data collected in the SIM registration. This shows the transparency of the act since it shows the specifics of how the data is being stored and used. By clearly explaining and defining the details of data processing, users will be informed of what is the personal information needed to proceed and comply with the SIM registration. Informed consent is a crucial aspect of privacy protection, and the availability of a privacy notice facilitates this process. Meanwhile, Section 10 (3)[28] states that end-users will be notified on the same day to confirm that their registration form has been successfully submitted and accepted. By promptly informing end-users about the status of their registration, it ensures transparency and accountability in the process. End-users can have confidence that their registration has been received and processed accurately, and that their personal information is being handled securely. By promptly notifying end-users, any discrepancies or inconsistencies in the registration process can be detected early on, preventing fraudulent activities or the misuse of SIM cards.

Rights of the Data Subject

The SIM Registration Act also complies with the Rights of the Data Subject detailed in Section 16 of Republic Act 10173 – Data Privacy Act of 2012 [29]on the basis of Section 10 (q) c of the NTC Memorandum[30] which states that the act must enable mechanisms that allow end-users to exercise their rights as data subjects under the DPA of 2012 which outlines the rights of a data subject regarding their personal information. This includes the right to be informed about whether their information is being processed and to receive specific information, such as the purpose, recipients, and storage period, before their information is entered into a processing system. They also have the right to access their personal information, correct any inaccuracies, and request the blocking or removal of their information if it is incomplete, outdated, false, or unlawfully obtained. If their information is used improperly, the data subject has the right to be compensated for any damages.

The compliance of this act is beneficial for several reasons:

- Protection of privacy - by informing individuals about the processing of their personal information and granting them rights such as access, correction, and blocking of their information, it ensures that their privacy is respected. This helps to build trust between individuals and the organizations handling their data.
- Transparency and accountability - providing individuals with detailed information about how their personal information will be processed promotes transparency. It holds personal information controllers accountable for their data handling practices and ensures that individuals have a clear understanding of how their information is being used.
- Data accuracy and detail - granting individuals the right to access and correct their personal information helps maintain accurate and up-to-date data. This benefits both individuals and organizations by ensuring that decisions made based on personal information are reliable and reflect the most accurate data available.

---

[28] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

[29] Data Privacy Act of 2012, Rep. Act No. 10173, (Aug. 15 2012) (Phil.), https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/

[30] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

- Individual control and empowerment - by giving individuals the ability to exercise their rights and make choices regarding their personal information, such as blocking or removing it when necessary, the SIM registration act empowers individuals and gives them greater control over their own data.
- Legal compliance - complying with the rights of data subjects is a legal requirement under the Data Privacy Act. By adhering to these provisions, organizations avoid legal consequences such as penalties and sanctions.

Confidentiality

The SIM Registration Act complies with the DPA in terms of confidentiality. Section 20 (5) of DPA[31] states that employees, agents or representatives of a personal information controller or the PTEs, in this case, who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information is not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

Section 9 of the SIM Registration Act[32] is its Confidentiality Clause that states that any information and data obtained in the registration process is kept confidential and cannot be disclosed to any person. The disclosure of the full name and address shall only be made: (a) in compliance with any law obligating the PTE to disclose such information; (b) in compliance with a court order or legal process upon finding of probable cause; (c) in compliance with Section 10; or (d) with the written consent of the subscriber.

Section 10 of the SIM Registration Act[33] states that the PTEs shall be required to provide information obtained in the registration process only upon the issuance of a subpoena by a competent authority pursuant to an investigation 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 commit a malicious, fraudulent or unlawful act. The relevant data and information shall be kept by the PTEs for ten (10) years from the time the end-user deactivates their mobile number.

In the NTC Memorandum, Sections 8, 10, and 11[34] put into detail the obligations of Public Telecommunications Entities (PTEs) and the confidentiality clause in the SIM registration. Section 8 states that all PTEs shall maintain their own database containing information required under the Act. The database shall strictly serve as a SIM Register to be used by PTEs to process, activate or deactivate a SIM or subscription and shall not be used for any other purpose. Section 10 states that the PTEs are obliged to: (a) maintain a register of the SIMs of their respective end-users and include the data of existing postpaid subscribers in the SIM register; (b) treat as absolutely confidential and not to disclose to any person any information and data obtained in the registration process. Section 11 adds to the confidentiality clause in the SIM registration where it shall take effect at the point of activation and continue even after deactivation of the SIM and for as long as the end-users' data is still retained by the PTEs.

---

[31] Data Privacy Act of 2012, Rep. Act No. 10173, (Aug. 15 2012) (Phil.), https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/

[32]Subscriber Identity Module (SIM) Card Registration Act, Rep. Act No. 11934, (Sept. 19, 2022) (Phil.), https://www.officialgazette.gov.ph/2022/10/10/republic-act-no-11934/

[33]Subscriber Identity Module (SIM) Card Registration Act, Rep. Act No. 11934, (Sept. 19, 2022) (Phil.), https://www.officialgazette.gov.ph/2022/10/10/republic-act-no-11934/

[34] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html

Security

The SIM Registration Act complies with the DPA in terms of security by way of Section 6(e) of the SIM Registration Act which states that PTEs are obliged and enjoined to include processes wherein the submitted information and data will be verified and confirmed. This ensures that the information provided in the SIM registration is accurate and authentic. This helps to prevent instances of identity theft and fraud, where someone may attempt to use false or stolen identities to register SIM cards for malicious purposes. Verifying the submitted information also helps in identifying and preventing the misuse of SIM cards for illegal activities such as terrorism, organized crime, or other illicit activities. By ensuring the accuracy of the information provided, the SIM registration process can assist law enforcement agencies in their efforts to track and investigate such activities.

Punishments

The SIM Registration Act complies with the DPA in terms of punishments and penalties. Section 11 of the act outlines the penalties for violating its provisions.

- Section 11(b) For breach of confidentiality. - The penalty of a fine shall be imposed upon PTEs, its agents or its employees who shall directly or indirectly reveal or disclose any information or data of an end-user obtained during the registration requirement under this Act, unless otherwise permitted by this Act or other laws;
- Section 11(c) For breach of confidentiality due to negligence. - The penalty of a fine shall be imposed upon PTEs, its agents or its employees who, due to negligence, shall reveal or disclose any information or data of an end-user obtained during the registration requirement of this Act.

These two provisions comply with Sections 25 and 26 of the DPA. Section 25(b) states that the unauthorized processing of personal sensitive information shall be penalized by imprisonment and a fine shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law. Section 26(b) states that accessing sensitive personal information due to negligence shall be penalized by imprisonment and a fine shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

Compliance with Constitution

Compliance with the DPA and its IRR is not enough. The SIM Registration Act and the NTC Memorandum must also not be considered unconstitutional. Particularly, it must not violate Sec. 3 of Article III or the Bill of Rights of the 1987 Constitution which states that the privacy of the correspondence and communication shall be made inviolable except upon the lawful order of the court or when public safety or order requires otherwise, as prescribed by law. The Bill of Rights was created to empower citizens with a tool to balance the power of the government. Any law that is noncompliant with the principles of the Bill of Rights is considered unconstitutional. The Supreme Court of the Philippines, acting as the final interpreter of the nation’s laws, provides, through jurisprudence, guidance as to how the laws of the land are to be implemented and abided by both officials and citizens alike. This section aims to demonstrate that the SIM Registration Act and the NTC Memorandum are indeed compliant with the Bill of Rights and how existing jurisprudence supports the provisions of the SIM Registration Act and the NTC Memorandum.

Bill of Rights Section III

The privacy of the communication and correspondence between individuals is still upheld by the SIM Registration Act and the NTC Memorandum. Although the identity of the person is linked with a SIM card, no one including state agents or the different entities in the PTE is allowed access to this information. As mentioned again in Section 9 of the SIM Registration Act and Section 11 of the NTC Memorandum, any information and data obtained in the registration process described under the Act shall be treated as absolutely confidential and shall not be disclosed to any person. The government cannot just immediately go looking at the database of the personal information linked with a SIM card number. There are legal steps that must be taken to ensure the validity of the disclosure of confidential information.

In Section 11 of the NTC Memorandum, it clearly defines the following guidelines that the disclosure of confidential information is allowed: (1) in compliance with any provisions set by the DPA to disclose such information, (2) in compliance with the court order or legal process upon finding probable cause, (3) a subpoena by a competent authority pursuant in an investigation with probable cause of believing that the mobile number is associated in the commission of a crime or unlawful act, and (4) with written consent of the end-user to waive their right of confidentiality. For the last part, it is important to note that the PTE cannot use the waiver of one's right as a requirement for users to subscribe to their service.

All these exceptions to the disclosure of confidential information are acceptable, reasonable, and all for the good of public safety. The main purpose of collecting personal information of owners of SIM cards is clearly mentioned in Section 11 which is to aid criminal investigators and the court in solving the cases where the identity behind the SIM mobile number is critical to solving the said case. These exceptions are in line with the government's efforts to ensure the safety and security of the public.

Furthermore, Sections 58 and 59 of the IRR of DPA have stated the serious imprisonment and fines one can face for the malicious and unauthorized disclosure of personal information, respectively. There are provisions in place to punish those who will disclose the information collected in the registration process which indicates that this information shall only be disclosed once the necessity of the situation calls for it. The information collected during the registration process must not be disclosed except in situations where there is a compelling reason to do so, such as in the investigation and prosecution of criminal offenses.

Finally, Section 22 of the NTC Memorandum stated that any doubt in the interpretation of any provision of this Memorandum Circular shall be construed in a manner that accords the highest respect for privacy, and liberally interpreted in a manner mindful of the rights and interest of SIM subscribers/end-users. While it is necessary to disclose confidential information in certain circumstances, it must be done in a way that upholds the privacy rights of SIM subscribers and end-users.

Ople v. Torres

On December 12, 1996, President Fidel V. Ramos signed Administrative Order (AO) 308, entitled "Adoption of a National Computerized Identification Reference System" which sought to establish a decentralized national computerized identification system to be used among the various agencies of the government. The administrative order, however, lacked a specific enumeration of the data to be collected and a provision on safeguards. The Administrative Order was struck down by the Supreme Court due to

its broadness, vagueness, and overbreadth. It was also made clear by the Supreme Court that it is not per se against the use of computers to accumulate, store, process, retrieve, and transmit data as long as it is done within the limitations established by the Constitution.[35]

The Ople case established that the government has the burden to show that a law or order is justified by some compelling state interest and that it is narrowly drawn. Though the argument for the creation of AO 308, which was to increase convenience in transacting with government agencies and reduce fraud in transactions with government agencies, was somewhat debatable, the lack of specificity on the data to be collected and lack of stringent safeguards to protect the privacy of the data subjects was what made the Administrative Order violative of the Right to Privacy.

In the case of the SIM Registration Act, it is both justified by compelling state interest and it is narrowly drawn. The SIM Registration Act was enacted due to the increasing incidence of crimes committed using the SIM cards and it aimed to both aid in the solution of cases involving these crimes and in deterring malicious actors from committing such crimes using the SIM card. Section 5 (a) of the Act also limits the information to be collected on natural persons to only the full name, date of birth, sex, address, and a valid identification document. Section 9 of the Act provides that the data collected will be treated with utmost confidentiality and would only be disclosed upon the issuance of a court order upon finding probable cause based on Section 10 of the Act and Section 12 of the NTC Memorandum, in compliance with laws requiring its disclosure upon compliance with the Data Privacy Act, or with the written consent of the data subject. There are also stringent security measures in place by the provision of Section 10 (12) of the NTC Memorandum where the registry information are secured, encrypted and protected at all times and comply with the minimum information security standards prescribed by the DICT consistent with internationally-accepted cybersecurity standards and relevant laws, rules and regulations. Section 11 provides for the penalties to be incurred upon violation of the Act.

Thus, with the safeguards in place to protect the privacy of the data subjects and the specificity of the enumeration of the data to be collected for the purposes of this Act, it could be argued that the SIM Registration Act is in full compliance with the Right to Privacy and is thus constitutional based on the ruling of the Supreme Court in this case.

Kilusang Mayo Uno (KMU) vs Director-General, National Economic Development Authority (NEDA)

On April 13, 2005, President Gloria Arroyo signed Executive Order (EO) 420, establishing the Unified Multi-Purpose Identification (UMID) System.[36] It sought to establish a unified ID system for the use of government agencies, including government owned and controlled corporations. Kilusang Mayo Uno (KMU) filed a petition before the Supreme Court praying for the Executive Order to be nullified and labeled unconstitutional due to (1) usurpation of legislative powers and (2) infringement of citizen's right to privacy. Addressing the contention on privacy, the Supreme Court deemed the lack of complaint to the ID systems existing before the Executive Order to hurt the position of the petitioners since the prior ID systems gave a "free hand" to the individual agencies to collect information they deemed necessary and the UMID would limit the number of data to be collected to only 14 and the number of data to be displayed in the card to only 8, as provided in Section 4 of the Executive Order. The Court also

[35] Ople vs Torres, G.R. No. 127685 (July 23, 1998) (Phil.)
[36] Kilusang Mayo Uno v. Director General, National Economic Development Authority, G.R. No. 167798 (Apr. 19, 2006) (Phil.)

noted that the data required in EO 420 is already being collected by the different government agencies that are providing ID documents to their clients. The Executive Order also provided safeguards in Section 6 of the Executive Order on how the data collected is to be processed. Thus, the Court upheld the validity and constitutionality of the assailed EO.

The KMU case, in contrast with the Ople case, gave an example of an order or law that would hold when concerns about privacy are to be raised. In contrast with AO 308, EO 420 has both the specificity of enumerating the data to be collected and the sufficient safeguards to protect the rights of citizens against government overreach.

Therefore, it could be argued that the SIM Registration Act is constitutional on the basis that it has both the specific enumeration of required data found on Section 5 of the Act and the safeguards on Sections 9 and 10 of the Act, and Section 12 of the NTC Memorandum. Another point is that the data that were to be collected in pursuance of the Act is already held by existing ID systems used by government agencies such as driver's license, passports, tax identification number (TIN), Social Security Number (SSS), and many more.

Whalen vs Roe

In the case KMU vs Director-General, NEDA, the majority opinion cited Whalen vs Roe[37] having "persuasive force for upholding the constitutionality of EO 420 as non-violative of the right to privacy." This case, too, can be applied to support the validity of the SIM Registration Act.

In *Whalen*, the Supreme Court of the United States upheld the validity of a New York law that requires physicians to prepare Schedule II drugs, the most dangerous class of legal prescriptions, in triplicate form with one (1) copy furnished to the State, to be stored in a central computerized database containing the name and address of the patients and the identity of the prescribing physician. The said law is assailed to infringe the right to privacy of citizens and impair the doctor-patient relationship between healthcare provider and the patient. The Court rejected this claim by stating that the disclosure of private health information is an essential part of modern medical practices even if it is unfavorable to the character of the patient. The Court further states that the disclosure of these health information to the State, who is responsible for the health of the community, does not immediately amount to an "impermissible invasion of privacy."

The law in contention in *Whalen* required the collection of sensitive health information that could injure the character of the data subject while the SIM Registration Law only requires information that is regularly required when transacting on a daily basis and which could not cause reputational harm on the data subject. The District Court of Southern New York stated, "it would seem clear that the State's vital interest in controlling the distribution of dangerous drugs would support a decision to experiment with new techniques for control." *Whalen* justified the collection of information by saying that it is a legitimate exercise of the State's police power, in the purpose of controlling the proliferation of dangerous drugs in the community. The SIM Registration Act could also be argued to be a legitimate exercise of the State's police power for the purpose of aiding law enforcement in reducing the incidence of crimes using SIM cards and to deter bad actors from causing harm using SIMs.

[37] *Whalen v. Roe*, 429 U.S. 589 (1977)

Countries Implementing SIM Registration

Mandatory SIM card registration is a regulatory policy that requires mobile network operators (MNOs) to collect and verify customers' identification credentials and personal information before activating a prepaid mobile SIM card in their name. This policy has been implemented in many countries around the world, with the aim of enhancing security and preventing the use of mobile services for criminal activities, such as terrorism and fraud.

As of February 2021, 157 countries have mandated prepaid SIM card registration policies.[38] This means that individuals who want to activate a prepaid SIM card in these countries must provide their identification documents and other personal information to their mobile network operator for verification purposes. Failure to comply with this policy may result in the individual being disconnected from mobile services by their mobile providers. Additionally, the implementation of this policy is also a testament to the fact that the idea of SIM registration is not new and has been explored by many countries worldwide. Therefore, it can be inferred that the SIM Registration Act and the NTC Memorandum are consistent with the global trend of mandating SIM card registration and are, in fact, a necessary step towards ensuring the safety and security of the general public.

The reasons for implementing mandatory SIM card registration policies may vary depending on the country. Some countries may implement this policy to combat terrorism or other criminal activities, while others may do so to improve public safety or protect consumer rights. Regardless of the specific reasons, mandatory SIM card registration policies are often seen as an effective way to prevent the misuse of mobile services and ensure that mobile networks are used for legitimate purposes.

Provided below are some additional examples of countries that have implemented mandatory SIM card registration.

Austria

A mandatory SIM card registration policy was introduced on January 1, 2019, requiring customers to register their prepaid SIM cards with the respective mobile network operators[39]. This policy was aimed at improving public safety and combating crime by enabling authorities to identify the owners of mobile numbers used in criminal activities. Under the new legislation, all existing prepaid SIM cards in Austria had to be registered before September 1, 2019, or they would be blocked by the mobile network operators. Customers were required to provide their identification credentials and personal information to their respective mobile network operators in order to register their prepaid SIM cards. The introduction of this mandatory SIM card registration policy in Austria followed similar policies implemented by other European Union countries, such as Germany, Belgium, and Italy. These policies were aimed at preventing terrorist activities and other criminal activities, which were facilitated by the use of anonymous prepaid SIM cards.

[38] Yongo, E., Lowe, C., & Theodorou, Y. (2021). Access to Mobile Services and Proof of Identity 2021. Groupe Speciale Mobile Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf?fbclid=IwAR3aW24HIb_BuEu0AqbDl4tzYYZy3odweCyhv1szTlDZ1sfAh_-ATB4BzZA

[39] Proposed Mandatory Registration of Subscriber Identity Modules (SIMs) used for Publicly Available Electronic Communications Services Regulations. (2018, August). Malta Communications Authority. https://www.mca.org.mt/sites/default/files/Public%20Consultation%20DOCUMENT%20-%20SIMs.pdf

Indonesia

The government implemented a mandatory SIM card registration policy in October of 2017, which requires individuals to provide their identification documents in order to obtain a SIM card[40]. Indonesian citizens are required to provide their mandatory ID card, known as Kartu Tanda Penduduk (KTP), while foreigners are required to provide their passport.[41] This policy was introduced in response to concerns about the misuse of mobile phones, such as for criminal activities like terrorism and fraud. By requiring identification documents for SIM card registration, the Indonesian government hopes to increase public safety and improve the traceability of mobile phone users. The policy is enforced by mobile network operators, who are responsible for verifying the identity and information provided by customers before activating their SIM cards.

Poland

In June 2016, the Polish government introduced a package of counterterrorism legislation that included a provision for mandatory prepaid SIM card registration.[42] The legislation prohibited the purchase of anonymous prepaid SIM cards and aimed to enhance security measures for two major international events that Poland was set to host in July 2016, the North Atlantic Treaty Organization (NATO) summit and World Youth Day. The government claimed that mandatory SIM card registration was necessary to prevent potential terrorist activities and other criminal activities that could be facilitated by the anonymity of prepaid SIM cards. Existing prepaid SIM card owners had until February 2017 to register their cards, or the cards would be blocked. This policy required mobile network operators (MNOs) to collect and verify customers' identification credentials and personal information in order to activate a prepaid mobile SIM card in their name. The customers were required to provide proof of their identity and address to the MNOs for the registration process to be completed successfully. The policy was aimed at preventing the use of mobile services for criminal activities, such as terrorism and fraud, and enhancing national security.

Belgium

In December 2016, Belgium introduced a new legislation that made it mandatory for all new prepaid SIM cards to be registered.[43] This was in response to the terror attacks that happened earlier that year in Brussels. The registration process requires users to provide their identification information, such as their name, address, and national registration number. The information is then verified by the mobile network operator to ensure that it is accurate. For users who had already purchased prepaid SIM cards before the new legislation came into effect, there was a six-month grace period for them to register their SIM cards that ended on June 7, 2017. Failure to comply with the registration requirement can result in the SIM card being blocked. The Belgian government sees mandatory SIM card registration as a necessary measure to prevent the use of mobile phones for criminal activities and to improve national security. The registration requirement also serves as a tool for law enforcement agencies to track down criminals and terrorists who use mobile phones to communicate. The introduction of

[40] Theodorou, Y., Okong'o, K., & Yongo, E. (2019). Access to Mobile Services and Proof of Identity 2019. Groupe Speciale Mobile Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf

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

[42] TeleGeography. (2016, July 25). Poland launches pre-paid SIM registration. CommsUpdate. https://www.commsupdate.com/articles/2016/07/25/poland-launches-pre-paid-sim-registration/

[43] TeleGeography. (2016a, May 17). Belgium to implement pre-paid SIM registration this year. CommsUpdate. https://www.commsupdate.com/articles/2016/05/17/belgium-to-implement-pre-paid-sim-registration-this-year/

mandatory SIM card registration in Belgium is part of a larger package of anti-terrorism legislation. This legislation includes measures such as increasing the number of police officers, improving intelligence gathering, and enhancing airport security. The Belgian government hopes that these measures will make the country safer and more secure for its citizens and visitors.

Hong Kong

Hong Kong, officially the Hong Kong Special Administrative Region (SAR) of the People's Republic of China which enjoys a high degree of autonomy as a part of China. As an autonomous region of China, Hong Kong has provided their own laws and they too, have their own SIM Registration Act in place. The Telecommunications Regulation took effect on 1 September 2021 to implement the Real-name Registration Programme for Subscriber Identification Module (SIM) Cards.[44] The Regulation requires that users should provide complete real-name registration for their SIM cards with their telecommunications service providers from 1 March 2022. Existing SIM cards which have not been registered by the deadline of 23 February 2023 can no longer be used afterwards.

With telephone scams and related crimes on the rise, the SAR government is taking a proactive approach to address this issue. A public consultation has been launched to gather feedback from the telecommunications industry, relevant stakeholders, and members of the public on the implementation of a robust real-name registration program for subscriber identity module (SIM) cards.[45] The proposed program seeks to bolster law enforcement efforts against cyber fraud activities by requiring users of prepaid SIM (PPS) cards to provide their personal information, including their name, date of birth, and identity document number, as well as a photocopy of their Hong Kong ID card or valid travel documents. The registration limit will be capped at three PPS cards per user, and this scheme has proven to be effective in other countries such as Japan, Thailand, and some European nations. By safeguarding public safety and promoting social harmony, this initiative will be a crucial step in the fight against telephone deception.

Mandatory SIM card registration policies have been implemented in many countries around the world, with the aim of improving security and preventing the use of mobile services for criminal activities. However, critics have expressed concerns about the impact of these policies on privacy and freedom of expression.

One of the main concerns is that mandatory SIM card registration enables governments to track citizens and suppress dissent. Critics argue that this can lead to violations of human rights and undermine democracy. Additionally, mandatory SIM card registration may pose a challenge to the affordability and accessibility of mobile services, particularly in developing countries where many people rely on prepaid SIM cards.

Despite these concerns, many countries continue to enforce mandatory SIM card registration policies. The GSMA Digital Identity programme, which tracks this trend, notes that while many countries mandating SIM registration maintain data protection and privacy frameworks, a significant proportion of countries are either considering introducing a data

[44] Real-name Registration Programme for Subscriber Identification Module (SIM) Cards. (2023, April 27). Office of the Communications Authority. https://www.ofca.gov.hk/en/consumer_focus/guide/hot_topics/sim_registration/index.html

[45] Sheng, Y. (2021, February 19). Real-name registration for prepaid SIM cards will help prevent crimes. Chinadailyhk. https://www.chinadailyhk.com/article/158085#Real-name-registration-for-prepaid-SIM-cards-will-help-prevent-crimes

protection and privacy framework or do not have one at all.[46] This suggests that more needs to be done to ensure that the implementation of mandatory SIM card registration policies is balanced with the protection of individuals' privacy and human rights.

Some governments have responded to these concerns by implementing measures to protect privacy and ensure data protection. For example, the European Union's General Data Protection Regulation (GDPR) requires companies to protect the personal data of EU citizens, including data collected during SIM card registration.[47] Similarly, the Indonesian government has implemented regulations to ensure that personal data collected during SIM card registration is protected.[48]

Overall, while mandatory SIM card registration may be an effective tool for improving security, it is important to ensure that it is implemented in a way that balances the need for security with the protection of individuals' privacy and human rights. This requires a commitment to data protection and privacy frameworks, as well as ongoing monitoring and evaluation of the impact of these policies on individuals and society as a whole.

[46] Yongo, E., Lowe, C., & Theodorou, Y. (2021). Access to Mobile Services and Proof of Identity 2021. Groupe Speciale Mobile Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf?fbclid=IwAR3aW24HIb_BuEu0AqbDl4tzYYZy3odweCyhv1szTlDZ1sfAh_-ATB4BzZA

[47] Proposed Mandatory Registration of Subscriber Identity Modules (SIMs) used for Publicly Available Electronic Communications Services Regulations. (2018, August). Malta Communications Authority. https://www.mca.org.mt/sites/default/files/Public%20Consultation%20DOCUMENT%20-%20SIMs.pdf

[48] Theodorou, Y., Okong'o, K., & Yongo, E. (2019). Access to Mobile Services and Proof of Identity 2019. Groupe Speciale Mobile Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf

CONCLUSION

After analyzing the facts and arguments presented, we have determined that Republic Act No. 11934 or the SIM Registration Act[49] and its implementing rules and regulations which is the National Telecommunications Commission Memorandum Circular No. 001-12-2022[50] are not unconstitutional.

In Section 3(1), Article III of the 1987 Constitution[51] explicitly provides 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.". There is a rise in text scams, phishing links, and even terrorism using unidentified numbers by end-users with criminal intent. With the pandemic happening, our personal info including our numbers have been passed around[52]. In this premise, it is lawful for the government to impose an act in which crimes that would be done through using SIM cards for communication would be swiftly punished with the help of fast identification or even deter them from happening in the first place. The SIM registration Act has a valid governmental objective in collecting personal information of SIM card holders.

The SIM Registration Act of the Philippines requires all users of mobile phone services to register their SIM's providing their personal identity along side a valid-government issued ID or document in order to directly tie that certain SIM card to a person's identity which would inevitably help in reducing and tracking down scams in such a way that it mitigates the following unlawful acts stated on the previous statement.

Since the SIM Registration Act explicitly invokes end users to register along with their credentials which would bind a person's identity to a certain SIM card it is of utmost importance that the Act complies with the Data Privacy Act of 2012 (DPA)[53] and its Implementing Rules and Regulations[54]. In our findings, The SIM Registration Act is able to comply with the requirements of the DPA in terms of protecting the privacy rights of the users which would serve as a proof that the Act is constitutional.

[49] Subscriber Identity Module (SIM) Card Registration Act, Rep. Act No. 11934, (Sept. 19, 2022) (Phil.), https://www.officialgazette.gov.ph/2022/10/10/republic-act-no-11934/
[50] National Telecommunications Commission, Rules and Regulations Implementing Republic Act No. 11934, Otherwise Known as the "Subscriber Identity Module (SIM) Registration Act", Mem. Circ. 001-12-2022, (Dec. 12, 22) (Phil.), https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html
[51] Const., (1987), art. III (Phil.)
[52] Piad, J. M. A., Tyrone Jasper C. (2022, September 7). Salceda suspects contact tracing as source of data leak. INQUIRER.net. https://newsinfo.inquirer.net/1659610/salceda-suspects-contact-tracing-as-source-of-data-leak
[53] Data Privacy Act of 2012, Rep. Act No. 10173, (Aug. 15 2012) (Phil.)
[54] Implementing Rules and Regulations of the Data Privacy Act of 2012, Department of Information and Communications Technology, 13 September 2016.