International Journal of Global Community
Volume VII No. 3 (November) 2024

SIM Card Number as Property Right of User: Privacy Data Perspective

Valeria Erika Sari Palilling

Faculty of Law, Hasanuddin University, Makassar

E-mail: valerika.study@gmail.com

Abstract.
The use of applications, especially financial apps and social media, requires a mobile phone number or SIM Card Number as the main prerequisite in operating the program. Mobile phone numbers are useful for synchronizing customers' personal data. This research aims to examine the ministerial regulation on the reuse of SIM Card numbers based on Personal Data Protection. This research is normative research conducted by examining various formal legal rules such as laws, regulations, international conventions, and literature containing theoretical concepts that are associated with the problems to be discussed in this study. The results of this study indicate that (1) the SIM Card Number Provider has absolute ownership rights over the number, and (2) the current law has not specifically regulated the reuse of SIM Card numbers from a privacy data perspective. Here, with the current use of financial technology and its relation to customer numbers, it is potentially easier to breach one's personal data resulting in material and immaterial breaches.

Keywords: Recycled SIM Card; Reused Number; Privacy Right

Introduction

The Indonesian digital economy surpassed all other ASEAN member states in size in 2021 (Sapulette & Muchtar, 2023). At the same time, this affected the post-Covid-19 digital economy's growth (Perekonomian, 2022). According to Nguyen (2023), the term "digital economy" describes the use of information technology to produce, modify, market, and consume goods and services that are founded on the creation of new jobs that generate income.

The ease with which consumers can access and acquire goods and services is driving changes in people's lifestyles that are becoming more and more reliant on the digital economy (Nandy, 2023). As a result of technological innovation, economic changes that were primarily linked to the Internet increased, laying the groundwork for the development of the digital economy (Bukht & Heeks., 2018). Businesses can function successfully and efficiently with the help of the Internet (Meyke Alvianieta Ali, 2019). Additionally, consumers can conduct digital transactions, which facilitates what is commonly referred to as financial technology (fintech) transactions (Elahi, 2009).

In practice, personal data is typically needed for fintech services to function (Subawa, 2020). Name, email address, and cell phone number are the most basic types of personal information that are asked for (Subawa, 2020). The phone number, also known as the Subscriber Identification Module Card (SIM Card), was acquired by trading with a telecommunicate operator. Since the majority of social network apps require a verified personal SIM card number to register for their services, the growing number of SIM card numbers has a connection to privacy rights. Well-known social media platforms like Instagram and TikTok use a user's mobile number to link their account profile and confirm their identity.

Warren and Brandeis defined the right to privacy as the right to be left alone (Warren & Brandeis, 1890). It indicates that a person has the capacity or right to manage his information, privacy, and other aspects of his life (Newell, 1985). People have the right to decide whether or not their information is shared with the public (Glancy, 1979). According to Warren and Brandeis (1890), there must be something definite and "private" that needs to be kept hidden from the public.

According to Minister of Communication and Information Technology Regulation Number 14 of 2018 regarding the National Telecommunication Fundamental Technical Plan, it is legal in Indonesia to reuse SIM card numbers. The phrase *"Penggunaan Ulang Nomor Pelanggan"* is used in Minister of Communication and Informatics Regulation No. 14 of 2018 regarding the Fundamental Technical Plan, but the phrase *"daur ulang nomor Pelanggan"* is translated into the English words "reuse" and "recycle" on the Telecommunication Service Provider's official website. Nevertheless, the definitions of these two terms differ when they are used. In the context of environmental law, reuse and recycling

are frequently employed. However, originally, reuse and reuse had a much broader meaning and applicability. "Reuse," according to the Black Law Dictionary, is the process of reusing a product, either fully or partially, without transforming it into a new item. On the other hand, "recycle" refers to the process of using previously used products, separating them, and then repurposing them in accordance with their prior uses. Because the law requires it to be done so, this study chose to classify it as "Reuse" rather than "Recycle."

It is not illegal to resell numbers that have passed the grace period. Reusing SIM card numbers, however, actually leads to infractions like identity theft, embezzlement, and compromised personal information belonging to previous owners. Bank accounts and social media accounts may be inaccessible to the owner of personal data. This is contrary to personal data protection and information as a privacy right, which is defined as the inherent right of an individual to obscure his private life from the public's view (Humble, 2020). In addition, the sale and purchase event between the operator and the customer that has occurred will give rise to responsibilities, transfer of rights, and obligations which will then be studied in this research to find out the implications for the right to privacy attached to the customer's number.

Problem Statements

a. Who is the owner after a SIM card number purchase transaction?
b. What are the implications of the current law governing SIM Card Numbers as property rights in terms of data privacy protection?

Research Method

The methodology used for this research is a combination of literature review and case study analysis. By conducting an extensive review of relevant academic publications, scholarly articles, reports, and legal documents to gain a comprehensive understanding of the ownership over the property right of a SIM Card Number after a transaction occurs and the current law regulating the reused of SIM Card number and its implication on privacy data. The literature review focuses on national and international legal frameworks, including policies related to SIM cards as property right from the privacy right perspective. It also reviews the state practice in regulating reuse of SIM Card Number. The case study analysis involves examining the impact of reuse of SIM Card Number in this fintech era, which challenges Indonesian government to adapting with the current situation to keep protecting privacy data over a person.

Discussion

A. Ownership of SIM Card Number

The reuse of customer numbers raises questions about the sale and purchase regulated in Article 1457 of the Civil Code.

"Jual beli adalah suatu persetujuan dengan mana pihak yang satu mengikatkan dirinya untuk menyerahkan suatu barang, dan pihak yang lain untuk membayar harga yang dijanjikan."(Sale and purchase is an agreement in which one party binds itself to deliver a good, and the other party to pay the agreed price – ed)

Furthermore, in the case of subscriber numbers, buying and selling activities are also carried out. However, regarding the transfer of ownership, it is necessary to review the nature of the object being traded. In civil law, objects are divided into tangible and intangible objects. Tangible objects are objects that can be touched, while intangible objects are those that cannot be touched, usually in the form of ownership rights.

In relation to SIM cards, title to tangible property occurs when the physical card of the mobile number is traded. This means there is a rights transfer between the provider and the new user. However, if the user does not use the phone number within the deadline period, the provider can take ownership of the number.

Unilateral transfer of rights is also reflected in abandoned land. The government can take away a person's land rights if the land is proven to be abandoned. However, in controlling abandoned land, there are several stages. These stages consist of evaluation, warning, and determination of abandoned land. If the notification remains unattempted until the above period ends, the person concerned will be given a written warning up to 3 times. If the third written warning is also not implemented, then the head of the agency determines it as an abandoned area. Thus, abandoned land can be controlled by the state.

However, in the case of a cell phone number, while the card is still physically in one's possession, the cell phone number is a separate part. This means that the reuse of a subscriber number is not a trade in the card, but in the number. Furthermore, referring to Article 1(1) of Law Number 28 of 2014 on Copyright, *"Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan."* (Copyright is the exclusive right of the creator that arises automatically based on the declarative principle after a creation is expressed in a tangible form, without prejudice to the limitations in accordance with the provisions of the laws and regulations – ed.)

In terms of ownership, Richard A. Mann & Barry S. Roberts argues that intellectual property refers to personal property that has a significant economic type (Mann & Roberts, 2005). However, the field of corporate intellectual property

rights implementation is different, where the company still can have control over its assets depending on the agreement.

The principle of sale and purchase break in a copyright refers to the agreement that requires the Creator to submit his Creation through payment in full by the buyer so that the economic rights to the Creation are transferred entirely to the buyer without time limit, or in practice known as sold flat (Ratnawati, 2019). However, upon approval of a contract, the service provider may have control over its products.

Referring to the terms and conditions of the official page of one of the providers in Indonesia, *Tri.co.id*, SIM Card ownership is owned by the corporation, in this case PT Indosat Tbk (TRI, 2022). Simultaneously, telecommunication regulations in Indonesia also regulate the right of telecommunication service providers to manage mobile phone numbers and be responsible for the distribution of these numbers.

In the European Union, there is a policy named Mobile Number Portability (MNP). MNP refers to when the customers have the right to keep their mobile phone number when switching service mobile phone (provider) (Buehler, Dewenter, & Haucap, 2005). In property rights perspective, MNP reallocates the property rights in mobile phone numbers from the provider to the customer. It aims to develop the competition in mobile telecommunication (Buehler, Dewenter, & Haucap, 2005). Conversely, in Indonesia, there is no policy pertaining to MNP, where the ownership over phone numbers is owned by the telecommunication authority, which is the Ministry of Communication and Information. The Ministry of Communication and Information gave a license to the provider to manage the deactivation number, therefore the customer did not have full rights over its phone number. The only close regulation is Fixed Number Portability (FNP), which applies to home numbers, where the mechanism is one number for a house.

The EU argues that "number portability is a key facilitator of consumer choice and effective competition in a competitive telecommunications environment" (Council, 2002). Under research conducted in the EU, MNP gave a benefit towards the customers, whether they ported their number or not. Besides that, MNP also gave impact on:

a. Avoid the cost of phone number changes.
b. Benefits of mobing to a more preferred operator.
c. Intensifiesd competition.
d. Avoided cost of finding changed numbers.
e. Increased investment in number value due to reallocation of property right.

Nonetheless, beside of the benefits offered by MNP, there are several obstacles were found. Firstly, the high cost of the implementation due to the high investment cost as the technical infrastructure on the routing system, the provider has to adjust their system to support port numbers to another provider. Secondly,

the decrease in switching fee income. Before the establishment of MNP, the provider can gain profit from customers who change their number. However, through MNP there is no switching number which impacts the source of provider income. Therefore these factors will lead the provider to the competitive in establishing offers and prices (Suresh, 2011).

As the challenges were found, several states are applying reuse or reassignment of phone number, which is more beneficial for providers, especially in the form of business purposes. However, this research found there are losses or damages due to the reuse of phone number are subjected towards the customer as its sensitive characteristic.

B. Analysis of Reusing SIM Card Number

a. Privacy Data International Legal Instruments

Historically, Resolution 2200A (XXI) in 1996 adopted by the UN General Assembly is the result of the Cold War, where states under its political compromise agreed to enact the International Covenant on Civil and Political Rights (ICCPR). The ICCPR is one of the international documents that become the most fundamental document in the regime of international human rights law, as well as its scope in protecting civil rights and politics (Arifin, 2017).

Besides that, the characteristic of ICCPR which is the universality has provided a strong foundation for the state to obey the rules set in the ICCPR. Therefore, ICCPR has been a part of customary international law (CIL). Article 17 of the ICCPR has regulated the right to privacy, where every person is subjected to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honor and reputation.

According to the CCPR General Comment, the right to privacy is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The state is obliged to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.

States parties to the Covenant the necessary attention is not being given to information concerning how respect for this right is guaranteed by legislative, administrative or judicial authorities, and in general by the competent organs established in the State. In particular, insufficient attention is paid to the fact that Article 17 of the Covenant deals with protection against both unlawful and arbitrary interference. That means that it is precisely in State legislation above all that provision must be made for the protection of the right outlined in that article. At present the reports either say nothing about such legislation or provide insufficient information on the subject.

The right to privacy as a fundamental right has been enshrined in Article 17 of the ICCPR. Under the CCPR General Comment of Article 17, the State must guarantee against interferences and attacks from natural and legal persons. Furthermore, this article mandates that the State enact laws and take other actions to forbid invasions of privacy ((HRC), 1998). Article 17(1) of the ICCPR states that:

"No one shall be subject to arbitrary interference with his privacy, family, home or correspondence, not to an unlawful attack upon his honor and reputation."

Here, the High Commissioner for Human Rights stipulated that the legal obligation imposed under this article requires the state to adopt measures to prohibit any interference and attacks against this right ((HRC), 1998). Furthermore, the term "unlawful" refers to no interference that can occur except the law regulates so. Simultaneously, an authorized interference met if the provision, aims, and objectives comply with the ICCPR. In the term of "arbitrary interference", conceptually it aims to guarantee that even if the interference provided for by law, the law must be in accordance with the provision, aims, and objectives of the ICCPR, particularly the right to privacy. Moreover, paragraph 2 stipulates that

"Everyone has the right to the protection of the law against such interference or attacks."

In retaining personal information on any data banks or other devices, whether by public authorities or private individuals or bodies, the domestic law must regulate the mechanism. This aims to ensure that the data leakage is not disseminated. Therefore, privacy can be defined as a fundamental (though not an absolute) human right that needs to be protected by the state.

b. Reuse of SIM Card Number in Indonesian Positive Law

Indonesia does realize the urgency to establish regulations for protecting personal data. Therefore, in 2022 Indonesia formalized a special regulation that discusses personal data protection, which is the Law 27/2022 concerning Personal Data Protection (PDP Laws). According to this law, personal data as privacy rights lie under the protection principle, the principle of public interest, the principle of balance, and the principle of accountability. These principles refer to Article 2 (2) of Regulation of the Ministry of Communication and Information Number 20/2016 determines that good personal data protection principles must be based, one of which is respect for personal data as confidential privacy under the provisions of statutory regulations. Furthermore, privacy is the freedom possessed by the owner of personal data to declare whether personal data is confidential or not confidential unless otherwise determined under statutory provisions.

Referring to the Minister of Communication and Information Technology Regulation Number 14 of 2018 concerning the Basic National Telecommunications Technical Plan, the reuse of customer numbers is permitted. Reuse of SIM Card Number is defined as a customer number that for one reason or the customer-owner

no longer uses another, must be used for other prospective customers who need it. However, the grace period between when the customer number is returned by the old customer/owner and when the number is given to the new customer is not less than 60 (sixty) calendar days. This is under the mandate stipulated under Article 15 of Law Number 36 of 1999 concerning Telecommunications, that telecommunications service providers are obliged to follow the technical provisions as regulated in the Basic Technical Plan through a Ministerial Decree. The reuse of prepaid card numbers is essentially carried out if several criteria have been met, including the grace period has passed, and the NIK and KK history on the invalid number must be deleted.

a. The grace period has passed

Recycling phone numbers is motivated by the maximum capacity in number combinations for ten to twelve-digit numbers. Moreover, the implementation of the customer number reuse policy also occurs because of the high costs of adding other digits to telephone numbers (Lee & Narayanan, 2021). According to *Telkomsel.com,* the active period for a prepaid card if the customer forgets to top up credit is 30 days (grace period). If within 30 days the customer has not topped up the credit, the number will enter a blocking period. At this stage, customers cannot use the Internet, telephone, or SMS. However, users can unblock within 60 days after being blocked. If the customer does not unblock, the card will expire (115 days). During the expiry period, users still have the right to reactivate the forfeited card within 115 days. However, if it has passed the expiry period, the card will enter a regeneration period to be ready to be produced and resold, so the user cannot use the card. The reactivation process is 60 days calculated from the last day of the expiry period (Telkomsel, 2024).

Practically, in the United States, the number recycling policy at mobile carriers is also implemented through the Federal Communications Commission (FCC), whereas the 47 C.F.R § 52.15 gave authority to the carriers to reassign after a specified period. Similarly, In Indonesia, the implementation of customer number reuse also regulates the carrier's authority to reassign customer numbers after the 60-day grace period has passed.

b. Phone Number requires to be Registered

Additionally, to continue monitoring the sale of prepaid card numbers, Article 1 of the Decree of the Indonesian Telecommunication Regulatory Agency Number 3 of 2018 concerning Prohibition of the Use of Population Data Without Rights and/or Unlawful for Prepaid Telecommunication Service Customer Registration regulates that each prepaid card customer only can register themselves for a maximum of three (3) customer numbers in each NIK and NKK.

However, the weakness of data verification when registering prepaid cards can be seen in Decision Number 46/Pid.Sus/2023/PN Slt. Where in this case, the Defendant was legally and convincingly proven guilty of manipulating personal

data by registering a starter card using someone else's NIK and NKK data, intending to obtain personal gain in the form of a bonus from the company. A similar case can also be seen in Decision Number 15/Pid.Sus/2021/PN Mnk, where the Panel of Judges stated that the Defendant had committed the criminal act by considering Article 51 paragraph (1) jo. Article 35 of Republic of Indonesia Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2018 concerning Information and Electronic Transactions jo. Article 55 (1) 1st of the Criminal Code. The data manipulation carried out by the Defendant brought losses because the starter card purchaser could act as someone else.

Although the NIK and NKK data have been deleted, the SIM Card number link in the application or account can make it easier for perpetrators to carry out hijackings (Lee & Narayanan, 2021). Based on a study conducted in 2014, (Bursztein, 2014) this type of data theft via recycling numbers can be categorized as manual hijacking. Manual Hijacking is defined as a non-automated effort to profile victims and maximize the profit or damage, which they can extract from a single credential (any sufficiently profitable credential will suffice) (Bursztein, 2014). Even though the number of cases tends to be fewer than hijacking via botnets or automated hijacking, the losses incurred are much more detrimental to the victims (Shay, Ion, Reeder, & Consolvo, 2014).

Generally, a SIM Card Number is well-known as a mobile phone number. Furthermore, the Global System for Mobile Communications Association (GSMA), a global association that works on global telecommunication has merged several basic principles in regulating pertaining to mobile privacy, which are:

a. Openness, transparency, and notice
b. Purpose and use
c. User choice and control
d. Data minimization and retention
e. Respect user rights
f. Security
g. Education
h. Children and adolescents
i. Accountability and enforcement

Firstly, the principles of openness, transparency, and notice mean that the operator is responsible for ensuring and providing clear, prominent, and newest information regarding the retention of personal data and data privacy. *Secondly*, in processing personal data, the operator has to provide legitimate business purposes, and the use of personal information must meet a legal obligation. *Thirdly*, customers or users can exercise meaningful choices and control their personal data. *Fourth*, any personal information must be protected by using reasonable safeguards appropriate to the sensitivity of the information. *Five*, the customers must be provided with privacy and security information and ways to protect their privacy.

Six, any platform that is directed to children and adolescents must ensure that the contents are in accordance with its applicable domestic law. *Lastly*, all responsible persons are accountable for ensuring these principles are met.

Conclusion

a. The ownership right of SIM Card number is regulated under Law No. 36 of 1999 concerning Telecommunication, which gives rights and obligations to telecommunication operators regarding the allocation and management of telephone numbers. This then leads operators to manage SIM Card numbers by applying that each customer number belongs to the company.
b. The buying and selling process that occurs between the provider and the customer is not give the ownership right to the customer. The right to using SIM Card number is temporary, as long as the number is actively used. This will give potential for data breach or any type of cybercrime as the development of society require people to having SIM Card Number as their personal identity.

Recommendation

a. The absolute ownership of customer numbers by operators as telecommunication service providers should be reviewed and adapted to the current fintech situation. The unification of the meaning of personal data and SIM Card number which is categorized as sensitive personal data should be enough to illustrate that, even if, the number needs to be resold after a grace period, the criteria to fulfill the "reuse of SIM Card number" should be more complex.
b. The government through relevant agencies and institutions can refer to regulations and policies carried out by other countries where in the case of switching operators, customers can without the need to transfer the number to a new number or known as Mobile Number Portability.
c. Cooperation or synergy between operators and the government also needs to be improved, so that the view of customer numbers is not limited to business opportunities due to increased market demand, but also to maintain privacy aspects as part of human rights. ***

References

Arifin, S. (2017). The Meaning and Implication of ICCPR Ratification to Religious Freedom in Indonesia. Advances in Social Science, Education and Humanities Research.

Buehler, S., Dewenter, R., & Haucap, J. (2005). Mobile Number Portability in Europe. Diskussionspapier, No. 41 Helmut-Schmidt-Universität - Universität der Bundeswehr Hamburg, Fächergruppe

Volkswirtschaftslehre. From https://nbn-resolving.de/urn:nbn:de:gbv:705-opus-19232

Bukht, R., & Heeks., R. (2018). Defining, Conceptualising and Measuring the Digital Economy. International Organisations Research Journal, 2. doi:10.17323/1996-7845-2018-02-07

Bursztein, E. (2014). Handcrafted fraud and extortion: Manual account hijacking in the wild. Proceedings of the 2014 conference on internet measurement conference, (p. 347). doi:10.1145/2663716.2663749

Council, D. 2. (2002). universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). Official Journal of the European Communities.

Elahi, S. (2009). Privacy and Consent in the Digital Era. ELSEVIER Information Security Technical Report, 113. doi:http://doi:10.1016/j.istr.2009.10.004

Glancy, D. (1979). The Invention of the Right to Privacy. Arizona Law Review. Vol. 21 (1), 2. From https://law.scu.edu/wp-content/uploads/Privacy.pdf.

(HRC), U. H. (1998). CCPR General Comment No. 16: Article 17 (Right to Privacy), the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. United Nations.

Humble, K. (2020). Human rights, International Law and the Right to Privacy. From https://gala.gre.ac.uk/id/eprint/29182/7/29182%20HUMBLE_Human_Rights_International_Law_and_the_Right_to_Privacy_%28AAM%29_2020.pdf.

Lee, K., & Narayanan, A. (2021). Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States. APWG Symposium on Electronic Crime Research (eCrime), 1-17. doi:10.1109/eCrime54498.2021.9738792

Mann, R. A., & Roberts, B. S. (2005). Business Law and The Regulation of Business. USA: Thomson South-Western West.

Meyke Alvianieta Ali, M. C. (2019). Consumer Legal Protection in Electronic Commerce Transaction. Estudiente Law Journal, 1(1), 205-222.

Nandy, D. (2023). Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns. Journal of Current Social and Political Issues, 15.

Newell, P. (1985). Perspectives on Privacy. Journal of Environmental Psychology, 87-105. doi:10.1016/0272-4944(95)90018-7

Nguyen, O. (2023). Digital Econoy and Its Components: a Brief Overview and Recommendations. Munich Personal RePEc Archaive (MPRA) Paper Np. 116110. From https://mpra.ub.uni-muenchen.de/116110/

Perekonomian., K. K. (2022). Digital Economy Acceleation in e-Commerce and Online Travel Becomes One of the Effective Strategies to Encourage National Economic Performance. HM.4.6/179/SET.M.EKON.3/4/2022. From https://ekon.go.id/publikasi/detail/4092/digital-economy-acceler

ation-in-e-commerce-and-online-travel-becomes-one-of-the-effective-strategies-to-encourage-national-economic-performance

Ratnawati, E. T. (2019). Akibat Hukum Perjanjian Jual Beli Hak Cipta Dengan Sistem Jual Putus (Sold Flat). Jurnal Widya Pranata Hukum, 1(2).

Sapulette, M., & Muchtar, P. (2023). Redefining Indonesia's Digital Economy. Economic Research Institute for ASEAN and East Asia, No. 2022-06, 1-2. From https://www.eria.org/uploads/media/policy-brief/FY2022/Redefining-Indonesia%E2%80%99s-Digital-Economy.pd

Shay, R., Ion, I., Reeder, R., & Consolvo. (2014). "My religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking. CHI 2014, One of a CHInd. doi:10.1145/2556288.2557330

Subawa, I. M. (2020). Protecting Personal Data in Financial Technology in Indonesia. International Journal of Business, Economics and Law, 22(1), 59-68.

Suresh, A. (2011). Mobile Number Portability – Opportunities and Challenges. International Journal of Management Research and Development (IJMRD), 1(1). From https://ssrn.com/abstract=3536135

Telkomsel. (2024). Jaga Masa Aktif Kartu. Telkomsel.com. From https://www.telkomsel.com/support/jaga-nomor

TRI. (2022). Syarat dan Ketentuan. Tri Indonesia. Retrieved October 7, 2024 from https://tri.co.id/syaratketentuan

Warren, S., & Brandeis, L. (1890). The right to Privacy. Harvard Law Review, 4(5), 193.