Asia Internet Coalition (AIC) Industry Submission on Subscriber Identity Module (SIM) Card Registration Act, Philippines

25 February 2022

To

- *Senator Grace L. Poe, Chairperson of the Senate Committee on Public Services*
- *Ramon M. Lopez, Secretary, Department of Trade and Industry (DTI)*
- *Emmanuel Rey R. Caintic, Office of the Acting Secretary, Department of Information and Communications Technology (DICT)*
- *Atty. John Henry D. Naga, Privacy Commissioner, National Privacy Commission (NPC)*
- *Mark Llandro L. Mendoza, Secretary General, House of Representatives, Republic of the Philippines*
- *Commissioner Gamaliel A. Cordoba, National Telecommunications Commission (NTC)*

On behalf of the Asia Internet Coalition (AIC) and its members, I would like to take this opportunity to submit comments and recommendations on the Philippines' Subscriber Identity Module (SIM) Card Registration Act ("Act"). AIC is an industry association comprised of leading internet and technology companies in the Asia Pacific region with a mission to promote the understanding and resolution of Internet and ICT policy issues.

We acknowledge the importance of this Act that outlines the key elements of the data protection framework, with an objective of having a safe and secure online environment. AIC has been very active in submitting industry recommendations on some of the key policy issues in Asia, details of which can be accessed here. In the backdrop of digitalization and growth of digital services across the world, the role of data has become more and more significant. This has given rise to concerns of informational privacy and the exercise of rights over personal data. Without a framework to govern these two subjects, no digital industry can be sustainable.

In this regard, we are grateful to be able to present the enclosed submission on the Act, and would like to respectfully request the Philippines Government to consider our recommendations. We look forward to our continued engagement with the government and in building a credible and globally consistent policy framework in the Philippines.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration. Importantly, we would also be happy to offer our inputs and insights on industry best practices directly through stakeholder meetings and discussions to help shape the dialogue for an effective privacy regime in the Philippines.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

General Comments and Overview

The provision in the recently ratified Subscriber Identity Module (SIM) Card Registration Act that mandates social media users to use their real names and phone numbers in creating accounts is problematic. More than 80% of the total population in the Philippines are active social media users as of January 2022. Social media is a convenient and accessible means of consuming content and communication especially since internet connectivity in the Philippines is often slow and unreliable. Restriction of access to services for those users in the Philippines who do not provide the required registration information will have a disproportionately negative impact to certain groups of users, including those without access to a mobile phone or those without access to ID documentation.

Firstly, the mandatory registration of SIM cards will undermine security and privacy interests by increasing the public and private sharing and matching of SIM users' information. Companies, third parties and the state empowered to create individual profiles and give access to vast amounts of user data, inevitably will increase the overall chances of data breaches. This is exacerbated by moving into biometric registration with fingerprints and facial recognition.

It is important to note that provision on social media registration was not indicated in House Act 5793 or Senate Act 2395, the Acts which Congress deliberated on before drafting the final version of the Act.[1] Information collected as part of mandatory registration, kept for an indefinite amount of time, used for different purposes and applied for secondary uses, including biometric databases, put individuals in particular vulnerable groups at risk of tracking and targeting, increasing the chances of their private information being misused. The experience of many countries clearly demonstrated the numerous ways through which criminals and rogue state actors regularly circumvent this type of regulation. Consequently, some countries that once considered adopting a similar system have either abandoned their attempts or steered clear of such aspirations entirely[2]. The registration requirement will also substantially impact individuals who use social media as a "safe space" to explore their identity, find support, and manage boundaries safely under a veil of anonymity. For example, social media has helped marginalized populations or groups excluded due to gender identity, sexual orientation, age, physical ability, and/or language to find their community of like-minded people.

Secondly, with the Act's vague scope and insufficient legislative guidelines, it projects an abundance of potential abuse scenarios if implemented. Mobile users will be asked to provide their personal data, including sensitive personal information, to third-party resellers—entities that would ordinarily have no business asking for such information. These entities are frequently ill-equipped to handle such amounts of data, making them more prone to data loss or misuse. Meanwhile, the system would

[1] https://www.philstar.com/headlines/2022/02/04/2158543/mandatory-sim-card-registration-puts-privacy-risk-might-not-curb-crime

[2] Mexico repealed in 2012 their law on the SIM registration, passed in 2009, after it was "found to be ineffective" and "created various new illicit and illegal activities such as black market SIM trading, SIM cloning, SIM spoofing, petty theft or robbery of phones for SIMs inside them". The European Commission of the European Union had concluded that "SIM registrations provided no benefit to assisting criminal investigations" of its member-states. https://mb.com.ph/2021/01/27/experts-warn-on-risks-of-mandatory-sim-card-registration/

afford the government easy access to the data collected while providing little to no limitation on its use.

Thirdly, there exists a lack of industry consultation, for the Act was not thoroughly deliberated upon and without consultation with relevant stakeholders. Therefore, we request the Government of the Philippines to review the Act, study the provisions further and conduct wider consultation with industry stakeholders – both on the provisions in the existing Act and associated implementing rules and regulations.

Although we appreciate the Philippines government efforts towards developing the Act, there are relevant concerns regarding its provisions that would significantly alter the landscape for digital companies. We strongly recommend that the Act should have more parity with the best practices to help improve compliance and improve business environment. It is useful and important to recognise that many of the ambitious conversations in this area are the subject of in-depth, evidence-based, and lengthy policy research and exchanges, where a panoply of policy solutions are being explored rather than a rushed legislative route.

Policy Issues and Recommendations

1. Maintaining users' freedom to remain anonymous online is vital

The Act seeks to remove anonymity on social media. However, there are benefits to anonymity. In repressive environments, anonymity serves as cloaks of protection to human rights defenders, journalists, members of political opposition, and marginalized groups.

Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.

We would like to emphasize the Inter-American Commission on Human Rights (**IACHR**) rapporteur[3] on exercising freedom of thought and expression, and protection of personal data and of anonymous speech.

- Article 19 of the Universal Declaration of Human Rights enshrines the right to freedom of opinion and expression, including the right to seek, receive, and impart information and ideas through any media. There can be no meaningful protection for citizens' freedom of expression if individuals lack the right to read and communicate anonymously. The right to seek and receive information is chilled when the government or others have unchecked access to records linked to viewing or reading habits of individuals.

[3] Annual Report of the Office of the Special Rapporteur for Freedom of Expression.Chapter IV (Freedom of Expression and the Internet). OEA /Serv.L/V/II.149. Para. 134.

- Anonymity is keeping confidential a wide variety of one's online activities including location, frequency of communications, and myriad of other information. Online anonymity is understood not only being unidentified and unknowable to third parties. It is incomplete to conceptualize the right to anonymity online simply as the right to freely participate in any online activity without disclosing one's name to anyone.

The Act can also potentially disenfranchise some marginalized sectors (women, LGBTQIA+, among others) who rely on social media to publish and seek help regarding their situation. The Act disregards human rights respect where in the Philippines and many parts of the world, people's lives would be at risk if they were not able to post anonymously - human rights defenders, dissidents, whistle-blowers, journalists, artists, people of certain faiths, and many others.

The ability to operate anonymously only supports safety for many users. This includes activists, political dissidents, people from minority groups, and journalists and their sources. In many scenarios – and across all geographies – some portion of any given population will likely be reluctant to speak freely or conduct their activities online without the protection of anonymity online. These include:

- People exploring their gender or sexuality
- People facing their own or a loved one's health crisis or mental illness
- Members of online forums dedicated to discussing sensitive personal finances

If real names should be required upon registration, at the very least, the Act should clarify that real names will not be published on social media platforms. Secondly, Civil societies, particularly human rights groups, must increase the public conversation regarding the Act and include this in the 2022 Philippine presidential debates.

Anonymity is critical for enabling democratic speech, whistleblowing, and for victims of physical and mental abuse to seek help. We have seen communities of individuals who have suffered domestic abuse come together, anonymously, because that is an important part of their ability to share their experiences.

We are also concerned about the compatibility of any proposed restrictions on anonymity with the duties of Category 1 providers under the Act to protect content of democratic importance, which rightly seeks to promote healthy democratic debate online.

Note the recent opinion[4] from the European Court of Human Rights, finding that the compelled unmasking of online commenters who criticized the Austrian government was a violation of freedom of expression.

We are of the view that preserving the right to remain anonymous online is an important part of preserving free expression in our society. In some parts of the world, people's lives would be at risk if they were not able to post anonymously.

Furthermore, Anonymity can be a form of protection. Posting anonymously allows people to protect themselves so that they are able to freely discuss and deal with complex topics safely. But the ability to be anonymous online does not come with consequences.

- Social media providers take action against pseudonymous accounts that violate their rules, policies and terms of services

[4] https://t.co/D761jPmcrW

- There is no empirical evidence that points to anonymity bans as ineffective. **(Refer to South Korea Case Study in Appendix A)**

Harassment and discrimination are social and cultural problems, not just online community problems, and we may achieve better results by focusing on changing climates of conflict and prejudice rather than removing anonymity.

2. Being anonymous or pseudonymous online does not give anyone the right to break local laws

The Act requires the use of real names upon account registration, thus implying that the use of pseudonyms is prohibited, even if such is the publicly known name of a user. The Act also puts much broader obligations and has negative effects on a wide group of communities, such as activists, members of the LGBTQIA+, celebrities, and other individuals known to use pseudonyms in public.

Therefore, we recommend reconsidering the blanket prohibition of the non-use of real names upon account registration, particularly if a user publicly uses a pseudonym. The use of pseudonyms is also a safety tool for users. The Act does not make any distinction on a valid use of pseudonyms, which should be allowed. Many first voices to speak about societal wrongdoings on social media have done so behind some degree of pseudonymity.

Where conduct or content is serious enough to be illegal, law enforcement agencies already have a range of legal powers to investigate – including seeking court orders to request subscriber or user data from the relevant service provider via due process and applicable lawful access regulations.

In addition, the Philippines has a wide body of statutes penalizing the use of fictitious/false names summarized in Executive Order No. 306 (Series of 2004) such as:

1. the Revised Penal Code which penalizes the public use of a fictitious name for the purpose of concealing a crime, evading the execution of a judgment or causing damage (1st paragraph, Art 178), the concealment of a person's true name and other personal circumstances (2nd paragraph, Art. 178), and the Act of defrauding another by using a fictitious name (4th paragraph, Art. 315);
2. Presidential Decree No. 1829, which penalizes any individual who shall knowingly or wilfully obstruct, impede, frustrate or delay the apprehension of suspects and the investigation and prosecution of criminal cases by publicly using a fictitious name for the purpose of concealing a crime evading prosecution or the execution of a judgment, or concealing his true name and other personal circumstances for the same purpose (Sec. 1[d]); and the Tax Reform Act of 1997 (RA8424), as amended, which made it unlawful for any person to enter any false or fictitious name in a taxpayer's books of accounts or records; and
3. Commonwealth Act No. 142, as amended by RA No. 6085, which allows a pseudonym solely for literary, cinema, television, radio or other entertainment purposes and in athletic events where the use of pseudonym is a normally accepted practice and penalizes any person who shall use any name different from the one with which he was registered at birth in the office of the local civil registry, or with which he was baptized for the first time, or with which he was registered in the Bureau of Immigration, or such substitute name as may have been authorized by a competent court (Sec. 1).

Individual end-users may also be able to seek remedies through civil actions.

3. **Broad scope of authorities which have the power to compel disclosure of registration information and the underlying acts as basis for their issuance violate Philippine users' right to due process of law**

The Act gives a broad number of government agencies access to users' registration information if they are duly authorized under existing laws to issue a subpoena. Administrative agencies' power to issue a subpoena is limited for the purpose of enforcing the laws they are authorized to administer - insofar as the Act effectively sanctions administrative investigations for "hate speech, trolling, spread of digital disinformation or fake news" which are not currently penalized or even defined under existing law, the Act may be infringing on the right to due process, since it does not provide a fair notice or warning to ordinary citizens as to what the unlawful conduct is. (The Act also mistakenly assumes that these acts are already "defined under pertinent laws.") Administrative agencies might seek to access user information even if they have no legal basis to investigate the matter at issue.

Further, "hate speech, trolling, spread of digital disinformation or fake news" all constitute speech. Since these acts are not yet defined, they may be susceptible to differing interpretations by ordinary citizens and law enforcers alike and, as a result, may have a chilling effect on protected speech. Statutes regulating speech may be challenged on the ground of vagueness or overbreadth. In Estrada v. Sandiganbayan, G.R. No. 148560, 19 November 2001, the Supreme Court stated:

> *A facial challenge is allowed to be made to a vague statute and to one which is overbroad because of possible "chilling effect" upon protected speech. The theory is that "[w]hen statutes regulate or proscribe speech and no readily apparent construction suggests itself as a vehicle for rehabilitating the statutes in a single prosecution, the transcendent value to all society of constitutionally protected expression is deemed to justify allowing attacks on overly broad statutes with no requirement that the person making the attack demonstrate that his own conduct could not be regulated by a statute drawn with narrow specificity." The possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that the protected speech of others may be deterred and perceived grievances left to fester because of possible inhibitory effects of overly broad statutes.*

In the same case, the Supreme Court stated that under the void-for-vagueness doctrine, a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law. On the other hand, the overbreadth doctrine decrees that a governmental purpose may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.

4. **The requirements of the Act effectively mandate overcollection of personal information, and are contrary to the privacy principles of the Data Privacy Act (DPA)**

The Data Privacy Act (DPA) applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing in the Philippines. Notably, Section 2 of the DPA states that "it is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth." This is further enshrined in Rule 1, Section 2 of the DPA's Implementing Rules and Regulations (IRRs).

Section 4 of the Act stipulates that real names and phone numbers be required upon social media account creation. There are no exceptions to Section 4, and all social media service providers (a term which is undefined under the Act) are to adhere to its provisions unconditionally. If mandated by law, such overcollection of personal information represents an avoidable and unnecessary intrusion into an individual's right to privacy. If such information (together with any other information about the individual on the applicable social media platform) is inadvertently compromised, then user information directly linked to a person's name and phone number could likely be used for state surveillance (particularly in connection with the Anti-Terrorism Act of 2020 and profiling for the imminent national elections), discrimination (most especially for social media platforms which process sensitive personal information such as sexual orientation or political affiliation), and identity theft and other cyber-security crimes (including SIM card cloning and social engineering), which further diminishes the user's human right of privacy. Instead, we invite further consideration of the data minimization principle where social media service providers should collect only what is directly relevant and necessary for their services instead.

Related to this point also is the principle of proportionality stated in Section 11(d) of the DPA and further enshrined by Rule IV, Section 18(c) of the IRRs. The principle of proportionality requires that personal data processing shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, and that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. After all, not every social media service provider requires an individual's name and phone number for the purposes of account creation, and many social media accounts can be created and be perfectly usable without such personal information ever being provided by users. Forcing social media service providers to collect such personal information without a business need is excessive and only serves to increase the service provider's compliance burden as the DPA's full set of obligations would apply to such information, without a corresponding positive business impact. Here, the requirement to collect a user's name and phone number is made even more burdensome by Section 10 of the Act, which requires the retention of such records for the excessive duration of ten years after deactivation of a user's account. Not only does this result in a significant increase in the volume of records which need to be appropriately maintained, the sheer amount of information available in these records also makes the social media service provider a far more attractive target to criminal activity. By way of comparison, the ten year period is double the five year obligation on Philippine banks to retain customer identification records and transactions documents following the closure of an account or the termination of the business relationship.

Particular attention should also be drawn to the purpose of the Act, which is to "deter the proliferation of SIM card, internet or electronic communication-aided crimes, such as, but not limited to: terrorism; text scams; unsolicited, indecent or obscene messages; bank fraud; libel; anonymous online defamation; trolling; hate speech, spread of digital disinformation or fake news as defined under pertinent laws." While there can be no disagreement as to the good intentions of the Act, it bears noting that many social media service providers already have in place sophisticated and privacy-protective security measures in place to combat and deter such crimes on their platforms. Even without an individual's name and phone number, the crimes that this Act seeks to prevent may still be reasonably prevented, investigated, and penalized by other equally effective means that do not require overcollection or retention for an unduly long period of time after service deactivation or account deletion.

5. **There are also many practical barriers to implementing such a regime as prescribed in the Act**

The way in which social media platforms verify people's identities would be challenging in practice, and may lead to government-run digital identity schemes which would be controversial. In addition, this could lead to fragmentation of the internet with users based outside the Philippines who are not verified having their content on platforms blocked to Filipino users.

Dedicated bad actors will always find ways to circumvent registration systems, including by using VPNs to mask their location (and therefore evade registration requirements focused on Philippine users) or by using other people's phone numbers to register for accounts. Moreover, statutes penalizing the use of fictitious names for the purpose of concealing a crime, evading the execution of a judgment or causing damage already exists (e.g., Section 178 of the Revised Penal Code and Section 1(d) of PD No. 1829).

Instead of introducing new user-facing obligations, the government should instead strengthen the capacity of law enforcers and improve inter-agency coordination. Rather than focusing on punishing trolls, resources could be dedicated to funding work being done by researchers and journalists on monitoring the information landscape and support civil society-led interventions to build frameworks for transparency.

6. Verification would disproportionately affect those without proper ID, as well as those who do not wish to sign up for accounts

This would be a significant barrier to a broad population of users who have a legitimate right to access this information. While other forms of ID could be accepted, it does illustrate the risk of creating a significant digital divide through enforced age gating. For instance, this is demonstrated through increasing the attainment gap between children from different socio-economic backgrounds, especially disadvantaging those in care. Consequently, the Act does not recognise the varying maturity levels of children at different age groups.

7. Adhere to principles of child protection

In not defining what social media is and what social media providers are, the Act is vague as to its coverage. There are websites/applications that are primarily online gaming platforms but have chat or sharing options. An example of this is Roblox which is "an online platform and storefront where users go to play games." Children also use it. Currently, there is no law setting the minimum age for social media use for children in the Philippines. Will children now be required to register their real names alone or together with their parents?

Therefore, the Act should define what social media is and who the social media providers are. It must also specifically consider the case of children or at least, those below 18 years old who use social media. With how it is currently written, the Act wants children and minors to disclose their real identities online. This may pose some challenges in keeping children and their identities safe.

8. Blanket penalties and fines should be avoided

We note that the Act aims to impose administrative penalties and fines. The Act imposes a high penalty of imprisonment of not less than 6 years or a fine of PHP 200,000 (USD 3,903, SGD 5,241) for the unauthorized sale of registered SIM cards. There are no graduations to the penalty.

The Act also penalizes users of not less than 6 years of imprisonment or fine of up to PHP 200,000 ((USD 3,903, SGD 5,241), or both for the use of fictitious identity in purchasing and registering SIM cards or social media accounts.

When imposing such sanctions, we would suggest that the Act must take into account the factors such as nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, any action taken to mitigate damage, the degree of responsibility of the public telecommunication entities (PTE) or a social media provider, any relevant previous infringements, the degree of cooperation with the regulator and other aggravating or mitigating factors. This aims to ensure that fines are properly tailored to the circumstances of the case at hand.

As an Act that not only regulates, but also penalizes, it must be clear on how it aims to impose the penalties. Blanket penalties should be avoided. According to Philippine penal law, crimes can be committed as follows: (1) attempted (2) frustrated, (3) consummated. The Act must clearly provide penalties commensurate to the gravity of the offense or the various modes of commission, (4)The Act unduly imposes a burden upon users when they choose not to disclose their real identities or the use of pseudonyms for security reasons. The Act does not make any distinctions for the valid use of pseudonyms.

It is further unclear what "information obtained in the registration process" includes (i.e., whether it is limited to the account holder's name and phone number or encompasses additional information). Depending on the scope of this data, social media providers may face conflicts of laws issues in responding to Filipino legal process seeking such data.

9. **Constitutionality**

The Act potentially violates the Constitutional rights of social media users.

a. Violation of right to privacy, in general

By requiring the collection of real names and phone numbers upon account creation by social media providers, the Bill arguably violates the right to privacy.

The 1987 Philippine Constitution provides that “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.”[5]

In Disini v. Secretary of Justice, G.R. No. 203335, 11 February 2014, the Supreme Court stated that "a law may require the disclosure of matters normally considered private but then only upon showing that such requirement has a rational relation to the purpose of the law, that there is a compelling State interest behind the law, and that the provision itself is narrowly drawn. In assessing regulations affecting privacy rights, courts should balance the legitimate concerns of the State against constitutional guarantees."

In this case, the relation between the mandatory collection of personal information by social media providers and the purpose of the Bill may be argued to be questionable. The declared purpose of the Bill in mandating the collection of personal information is "to deter the proliferation of SIM card, internet or electronic communication-aided crimes, such as, but not limited to: terrorism; text scams; unsolicited, indecent or obscene messages; bank fraud; libel; anonymous online

[5] 1987 Constitution, Article II, Sec. 3 (1).

defamation; trolling; hate speech, spread of digital disinformation or fake news as defined under pertinent laws." Notably, "trolling; hate speech, spread of digital disinformation or fake news as defined under pertinent laws" are not yet criminalized or even "defined under pertinent laws." Further, while Section 4(c)(3) of the Cybercrime Prevention Act previously penalized unsolicited commercial communications or "spam," the Supreme Court struck down the provision in Disini for being unconstitutional. In effect, there is likewise no law at the moment criminalizing "unsolicited … messages." As such, in relation to these acts, the mandatory collection of personal information does not have any bearing on the purpose of the Act to deter "SIM card, internet or electronic communication-aided crimes."

For the same reason, since "hate speech, trolling, or spread of digital disinformation, or fake news" are not yet criminalized or even "defined under pertinent laws," the grant of powers to "competent authorities" under Section 10 of the Act to investigate and compel the disclosure of personal information in relation to these acts is incongruous. In effect, Section 10 improperly authorizes investigation of non-criminal acts. At best, this would result in investigation without any prospect of prosecution. At worst, it may give way to excessive regulation of legitimate speech and conduct.

A further flaw in Section 10 is that while it refers to "hate speech, trolling, or spread of digital disinformation, or fake news" (which, again, are non-criminal acts), it does not expressly refer to "terrorism; text scams; unsolicited, indecent or obscene messages; bank fraud," which (except for "unsolicited … messages") actually constitute criminal offenses.

As for "terrorism; text scams; unsolicited, indecent or obscene messages; bank fraud; libel; anonymous online defamation," these may be committed even without social media. Indeed, by definition, "text scams" cannot be committed through social media. As for the others, they are likely to be committed outside social media.

Further, mandatory collection of personal information from all social media account users is not narrowly tailored for achieving the purpose of the law. In fact, behavior amounting to "terrorism; text scams; unsolicited, indecent or obscene messages; bank fraud; libel; anonymous online defamation" is the exception in social media. The vast majority of users who do not use their real names have legitimate reasons for doing so (e.g., to minimize safety risks, to escape retaliation for lawful online activity, such as criticism and expression of opinions and grievances). Yet, they are still covered by the Bill.

Notably, a narrowly tailored approach to the problem already exists in Philippine statute books. Thus, there are already laws penalizing the use of fictitious names for the purpose of concealing a crime, evading the execution of a judgment, or causing damage (e.g., Section 178 of the Revised Penal Code and Section 1(d) of PD No. 1829). Further, courts already have the power to intrude upon a person's right to privacy under Section 3(1), Article III of the 1987 Constitution (as further discussed below).

In Disini, the constitutionality of Section 12 of RA No. 10175, or the Cybercrime Prevention Act of 2012, which allowed law enforcement authorities "with due cause" to collect anonymous traffic data, was challenged. The Supreme Court struck down the provision on the ground that it violates the right to privacy, because "[t]he authority that Section 12 gives law enforcement agencies is too sweeping and lacks restraint. While it says that traffic data collection should not disclose identities or content data, such restraint is but an illusion. Admittedly, nothing can prevent law enforcement agencies holding these data in their hands from looking into the identity of their sender or receiver and what the data contains. This will unnecessarily expose the citizenry to leaked information or, worse, to extortion from certain bad elements in these agencies." In this case, the Act specifically

requires the disclosure of identities. There is, therefore, more reason to invalidate the same based on the right to privacy.

Under the Bill, PTEs and social media providers are required to retain user information for 10 years from the time of deactivation.[6] This also constitutes an unlawful interference with the right to privacy.

There is no relationship between the data whose retention was provided for a period of 10 years and a threat to public security. (**Refer to Digital Rights Ireland v Minister of Communications and Others in Appendix A)** By way of comparison, the ten year period is double the five year obligation on Philippine banks to retain customer identification records and transactions documents following the closure of an account or the termination of the business relationship.

b. Violation of right to privacy of communication and correspondence

Section 3(1), Article III of the 1987 Constitution mandates that "[t]he 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."

Except as regards terrorism, there is basis to argue that the Bill is not the "law" contemplated under Section 3(1). In his Concurring and Dissenting Opinion in Disini, Justice Carpio stated:

"When the members of the 1971 Constitutional Convention deliberated on Article III, Section 4(1) of the 1973 Constitution, the counterpart provision of Article III, Section 3 (1) of the 1987 Constitution, the phrase "public safety or order" was understood by the convention members to encompass "the security of human lives, liberty and property against the activities of invaders, insurrectionists and rebels." This narrow understanding of the public safety exception to the guarantee of communicative privacy is consistent with Congress' own interpretation of the same exception as provided in Article III, Section 1(5) of the 1935 Constitution. Thus, when Congress passed the Anti-Wiretapping Act 68 (enacted in 1965), it exempted from the ban on wiretapping "cases involving the crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage and other offenses against national security" (Section 3). In these specific and limited cases where wiretapping has been allowed, a court warrant is required before the government can record the conversations of individuals.

"Under RA 10175, the categories of crimes defined and penalized relate to: (1) offenses against the confidentiality, integrity and availability of computer data and systems (Section 4 [a]); (2) computer-related offenses (Section 4 [b]); (3) content-related offenses (Section 4 [c]); and (4) other offenses (Section 5). None of these categories of crimes are limited to public safety or public order interests (akin to the crimes exempted from the coverage of the Anti-Wiretapping Law). They relate to crimes committed in the cyberspace which have no stated public safety or even national security dimensions. Such fact takes Section 12 outside of the ambit of the Privacy of Communication Clause."

[6] SIM Card Registration Bill, Section 10.

Similar to the provision of RA 10175, except for terrorism, the activities which the Bill seeks to prevent "have no stated public safety or even national security dimensions."

c. Violation of freedom of speech and of the press

The Bill regulates speech in two ways:

(a) It proscribes anonymity in social media.

(b) It effectively authorizes investigation by law enforcement agencies (as opposed to courts only) of "hate speech, trolling, or spread of digital information, or fake news," which are not yet defined and penalized under existing law.

Arguably, anonymity can be a fundamental component of freedom of speech. In McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995), the US Supreme Court (the decisions in constitutional cases of which are persuasive in the Philippines), "[u]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority." The ruling may be reasonably applied to expression in social media.

As we previously noted, "hate speech, trolling, spread of digital disinformation or fake news" all constitute speech. Since these acts are not yet defined, they may be susceptible to differing interpretations by ordinary citizens and law enforcers alike and, as a result, may have a chilling effect on protected speech. Statutes regulating speech may be challenged on the ground of vagueness or overbreadth. In Estrada v. Sandiganbayan, G.R. No. 148560, 19 November 2001, the Supreme Court stated:

"A facial challenge is allowed to be made to a vague statute and to one which is overbroad because of possible "chilling effect" upon protected speech. The theory is that "[w]hen statutes regulate or proscribe speech and no readily apparent construction suggests itself as a vehicle for rehabilitating the statutes in a single prosecution, the transcendent value to all society of constitutionally protected expression is deemed to justify allowing attacks on overly broad statutes with no requirement that the person making the attack demonstrate that his own conduct could not be regulated by a statute drawn with narrow specificity." The possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that the protected speech of others may be deterred and perceived grievances left to fester because of possible inhibitory effects of overly broad statutes."

In the same case, the Supreme Court stated that under the void-for-vagueness doctrine, "a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law." On the other hand, the overbreadth doctrine decrees that "a governmental purpose may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms."

The observations of Chief Justice Sereno in her Concurring and Dissenting Opinion in Disini is instructive:

"One begins to see at this point how the exercise of freedom of speech is clearly burdened. The Court can take judicial notice of the fact that ICTs are fast becoming the most widely used and accessible means of communication and of expression. Educational institutions encourage the study of ICT and the acquisition of the corresponding skills. Businesses, government institutions

and civil society organizations rely so heavily on ICT that it is no exaggeration to say that, without it, their operations may grind to a halt. News organizations are increasingly shifting to online publications, too. The introduction of social networking sites has increased public participation in socially and politically relevant issues. In a way, the Internet has been transformed into "freedom parks." Because of the inextricability of ICT from modern life and the exercise of free speech and expression, I am of the opinion that the increase in penalty per se effectively chills a significant amount of the exercise of this preferred constitutional right."

The foregoing also applies more forcefully when the freedom of the press is involved, relating as it is to constitutionally protected journalistic activity.

d. Violation of right against unreasonable search and seizures

In People v. Chua Ho San, G.R. No. 128222, 17 June 1999, the Supreme Court indicated that "intrusions" upon "the inviolable right to privacy of home and person" require a valid search warrant, viz:

"Enshrined in the Constitution is the inviolable right to privacy of home and person. It explicitly ordains that people have the right to be secure in their persons, houses, papers and effects against unreasonable searches and seizures of whatever nature and for any purpose. Inseparable, and not merely corollary or incidental to said right and equally hallowed in and by the Constitution, is the exclusionary principle which decrees that any evidence obtained in violation of said right is inadmissible for any purpose in any proceedings.

The Constitutional proscription against unreasonable searches and seizures does not, of course, forestall reasonable searches and seizure. What constitutes a reasonable or even an unreasonable search in any particular case is purely a judicial question, determinable from a consideration of the circumstances involved. Verily, the rule is, the Constitution bars State intrusions to a person's body, personal effects or residence except if conducted by virtue of a valid search warrant issued in compliance with the procedure outlined on the Constitution and reiterated in the Rules of Court; "otherwise such search and seizure become "unreasonable" within the meaning of the aforementioned constitutional provision."

Further, In the Matter of the Petition for Issuance of Writ of Habeas Corpus of Camilo L. Sabio, G.R. No. 174340, 17 October 2006, suggests that such right to privacy includes a person's "right to be let alone" or the "right to determine what, how much, to whom and when information about himself shall be disclosed."

It may be argued that the wholesale collection of personal information mandated by the Bill rises to the level of a search and seizure. Under Section 2, Article III of the 1987 Constitution, the issuance of a search warrant requires "probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized." Insofar as the Bill does not comply with this requirement, and even allows persons and agencies other than judges to authorize access to personal information (in connection with an investigation of supposed crimes), it violates the right against unreasonable search and seizures.

e. Violation of the equal protection clause

In requiring collection of real names and phone numbers upon social media account creation, the Bill creates a classification based on use of social media. Classification, to be valid, must: (a) rest on substantial distinctions; (b) be germane to the purpose of the law; (c) not be limited to existing conditions only; and (d) apply equally to all members of the same class.

In this regard, Commonwealth Act No. 142, as amended, allows the use of "a pseudonym solely for literary, cinema, television, radio or other entertainment purposes and in athletic events where the use of pseudonym is a normally accepted practice." Further, Article 379 of the Civil Code states that "[t]he employment of pen names or stage names is permitted, provided it is done in good faith and there is no injury to third persons" (Tiu v. Court of Appeals, G.R. No. 127410, 20 January 1999).

Activities in social media may be characterized as for "literary, cinema, television, radio or other entertainment purposes." However, only on the basis that social media is used for such activities, the Bill requires the disclosure of personal information. In doing so, it may be argued that the Bill violates the equal protection clause.

We are aware of the ruling in Disini that "there exists a substantial distinction between crimes committed through the use of information and communications technology and similar crimes committed using other means. In using the technology in question, the offender often evades identification and is able to reach far more victims or cause greater harm. The distinction, therefore, creates a basis for higher penalties for cybercrimes." However, Disini dealt with criminal activities, while the large swathes of social media activities are not criminal in nature.

10. The overly broad coverage of the Act, as a result of the lack of definition of "social media providers", violates the right to privacy

The right to privacy is a fundamental right guaranteed by the Constitution and it is the burden of the government to show that an intrusion upon it is justified by some compelling state interest and that it is narrowly drawn. The Act, in imposing an obligation on social media providers to require real-names and phone numbers upon account creation, fails to define what a social media provider is. In this information age, where internet access is as ubiquitous as cars on the road, the broad scope of the Act could be tantamount to a state surveillance of an individual's online activities.

Social media covers a broad spectrum of services offered online, ranging from blogs, business networks, collaborative projects, photo sharing, video sharing, social networks, and virtual worlds, among others. In addition, not all social media companies have a physical and juridical presence in the Philippines.

Requiring Philippine users to give their real names and phone numbers before availing any of these services might not only be unnecessary to prevent the evils the Act seeks to prevent, it also reaches into online private spaces where individuals should have a reasonable expectation of privacy. In Disini v. Secretary of Justice, G.R. No. 203335, 11 February 2014, the Supreme Court stated that "a law may require the disclosure of matters normally considered private but then only upon showing that such requirement has a rational relation to the purpose of the law, that there is a compelling State interest behind the law, and that the provision itself is narrowly drawn. In assessing regulations affecting privacy rights, courts should balance the legitimate concerns of the State against constitutional guarantees." Exceptions to the right of privacy should be upheld only if they represent "compelling State interest" and even then, should be narrowly interpreted. In our view, this is fulfilled if disclosure may be compelled only in connection with the investigation of criminal offenses. It may be argued that proceedings other than these primarily consist of actions to enforce private interests.

Requiring the disclosure personal information to PTEs and social media providers may be said to be excessive considering the purpose of the Act "to deter the proliferation of SIM card, internet

or electronic communication-aided crimes, such as, but not limited to: terrorism; text scams; unsolicited, indecent or obscene messages; bank fraud; libel; anonymous online defamation; trolling; hate speech, spread of digital disinformation or fake news as defined under pertinent laws." Notably, at present, some of these acts are not even defined as crimes. In any case, they may still reasonably be prevented, investigated, and penalized by other means and not solely by requiring the disclosure of social media account users' names and phone numbers.

While there can be no disagreement as to the good intentions of the Act, its sweeping coverage should be given a second look to preserve the mantle of protection upon one's person and their right to privacy as is guaranteed by the Constitution. The compromise between the preservation of our Constitutionally enshrined liberties and national security, if one is to ever be made, should always be ruled in favor of the former.

We therefore recommend that the Act should take out the requirements on social media providers out as this is a SIM Card Act. In the interest of adding the social media providers in the Act, these stakeholders should be invited for the hearing and the definition should be added in the Act of what social media is and who the social media providers are.

11. No one-size fits all solution to ensure authenticity in social media

The digital industry is highly innovative and diverse, and digital platforms like social media providers operate vastly different businesses which offer a wide and constantly evolving variety of services and products. Social media providers have different models of representation: some platforms are designed for users to share with known persons/identities while others let users share more creatively with a broader audience.

There is no one-size fits all solution to ensure authenticity in social media. Social media providers should be given the flexibility to respond in a way that best matches their business model, risk profiles, technical limitations, and available resources. The specifics of policies, systems, processes, resourcing and other provisions should not be mandated.

To preserve freedom of expression, social media providers should be allowed to continue to offer individuals a range of diverse ways to express their identity while also preventing impersonation and identity misrepresentation. Authentication should at all times be tailored to the specific risk seeking to be mitigated and proportionate in impacting the users implicated in the risk.

In this regard, we are grateful to be able to present our concerns on the same, and would also like to restate our continuous support and assistance to the Philippine government in its efforts to bring about this transformational change. We look forward to our continued engagement with the government and in building a credible and globally consistent policy framework in the Philippines.

Appendix A

South Korea case study: In 2004, the South Korean government passed a law requiring users to provide their national identification numbers before posting on election-related websites. Studies have shown that at the time the policy was in effect, there was no significant decrease in online abuse. In

fact, the Korean Communications Commission found that 'hateful' comments decreased by less than 1% during the first year the policy was in force. Other studies found short-term decreases in online participation and the number of violent comments, but saw no long-term changes. The policy doesn't appear to have prevented the spread of misinformation or conspiracy theories. What happened though was a massive hack that stole 35 million South Koreans' national identification numbers.

- The 2021 January ruling by the Constitutional Court confirmed that the proposed limit to freedom of expression based on anonymity will:

    - create undue self-censorship fearing any political retaliations
    - limit the exchange of diverse opinions on the Internet, and therefore, freeze the free expression of ideas and opinions of the Korean people;
    - and ultimately hamper the formation of free public opinions, which is the basis of democracy.

- This case was made for specific election periods, however, the Court noted that there are mediation mechanisms available and can be leveraged including the Communications Standards Commission specifically for elections -- instead of resorting to a mandatory real-name policy.[7]

- **Bailey Poland, a researcher in online abuse lays this out eloquently:** "The ability to access the Internet and communicate with one another in anonymous ways, however, is an important part of a free and open Internet. There are numerous valid reasons people may wish to be anonymous— for example, transgender persons who have not yet come out to their family or community may want the ability to ask questions without their being connected to existing online profiles. A woman attempting to escape an abusive relationship may reach out anonymously for help. Political dissent in a number of regions and countries must be expressed anonymously to avoid state repercussions or retribution from other citizens." (Poland, B. (2016). DEALING WITH CYBERSEXISM: Current Solutions. In Haters: Harassment, Abuse, and Violence Online (pp. 159-200))

- **In 2015, researcher Sarah Gunther Being argued that Facebook's "Real Name" Policy was a violation of the corporate responsibility to respect Human Rights.** Her paper outlines why being able to control one's identity and expression online is a fundamental precondition to the protection and exercise of human rights and a key component of online safety for queer, trans, youth and other communities. It also examines some important distinctions between anonymity and pseudonymity.

- These complexities have been echoed by cyber-hate researcher and journalist Ginger Gorman who acknowledges that anonymity bans are a simplistic approach that does not get to the core social issue.

- **Breach of the rights to privacy and data protection**. In Digital Rights Ireland v Minister of Communications and Others, the Grand Chamber of the Court of Justice of the European Union (CJEU) concluded that the 2006 Data Retention Directive, which required communications service providers to retain consumer data for up to two years for the purpose of preventing and detecting serious crime breached the rights to privacy and data protection. **The CJEU observed that the scope of the data retention "entails an interference with the fundamental rights to practically the entire European population."** THe CJEU further noted that the Directive was flawed for not requiring any relationship between the data whose

[7] https://ccnews.lawissue.co.kr/view.php?ud=2021042913305832049a8c8bf58f_12

retention was provided for and a threat to public security. It concluded that the Directive amounted to a "wide-ranging and particularly serious interference with the rights to privacy and data retention without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary." The full judgment is available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf