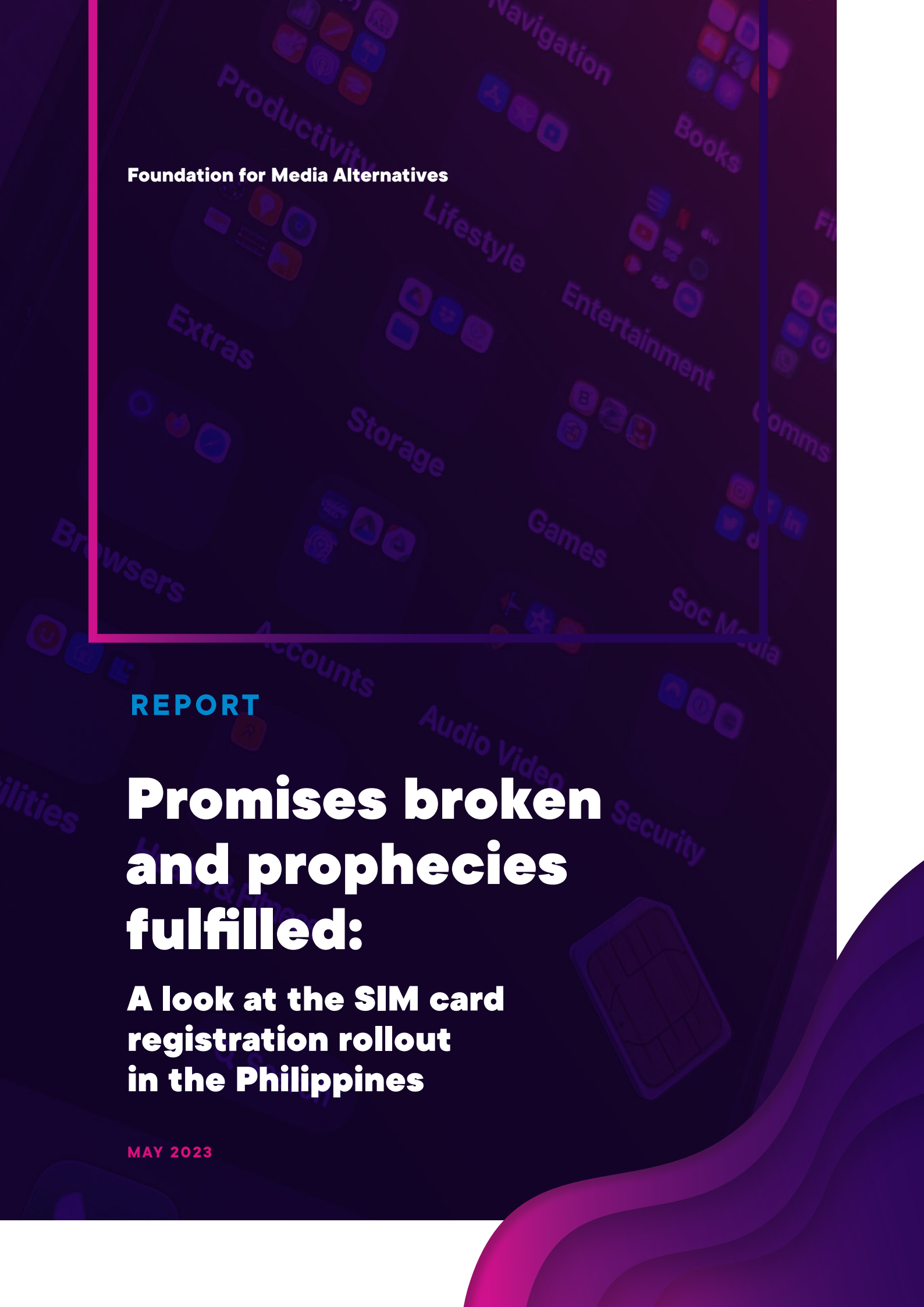




Foundation for Media Alternatives

REPORT

Promises broken and prophecies fulfilled:

**A look at the SIM card
registration rollout
in the Philippines**

MAY 2023

FOUNDATION FOR MEDIA ALTERNATIVES

2023

Published by the Foundation for Media Alternatives

29-P Matimtiman Street, UP Teacher's Village, Quezon City

T. (632) 7 356 7965

E. info@fma.ph

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike
2.5 Generic License.

To view a copy of this license, visit: <https://creativecommons.org/licenses/by-nc-sa/2.5/> or
send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Stock photos courtesy of Envato Elements.

Promises broken and prophecies fulfilled:

A look at the SIM card registration rollout in the Philippines

About this Report

This report is a follow-up to a 2018 [briefing paper](#) published by FMA regarding mandatory SIM card registration. Released months after the rollout of the SIM Card registration system in the Philippines, it investigates how the measure is faring in relation to its promised benefits, as well as the risks and dangers its opponents have consistently warned about.

In 2022, less than two months before the eighteenth Congress of the Philippines ended its term, then President Rodrigo Duterte surprised everyone when he vetoed the SIM card registration bill that had already been approved by both chambers of the legislature. That measure would have required Filipinos and Philippine residents to register with the government both their SIM cards and social media accounts.

And so, instead of being this momentous conclusion of a successful campaign, that moment became just another close call for SIM card registration proponents who had already seen their efforts thwarted many times over these past couple of decades. Indeed, this was not their first attempt. One of the earliest proposals dates back to 2004, [filed by former Senator Rodolfo Biazon](#). Since then, each Congress has seen at least one similar bill brought up for consideration.

In 2018, we published a [briefing paper](#) on the risks and implications of a mandatory SIM card registration system. There, we made sure to emphasize those issues relating to the individual right to privacy and data protection. Today, there is a need to revisit and update that guidance document because of major developments that have transpired since its release.

As of this writing, April 2023, the Philippines has formally embraced SIM card registration with the enactment of Republic Act No. 11934, also known as the “Subscriber Identity Module (SIM) Card Registration Act”. Current President, Ferdinand Marcos, Jr., signed the law on 10 October 2022, after it hurdled the legislative process in record speed. It was the first law that Marcos Jr. signed as President.

Most sectors welcomed the news with open arms. For core supporters, it signaled the alignment of the domestic regulatory landscape with the global context and saw the country joining the majority of its peers that already require SIM card registration. According to [a non-commissioned nationwide survey](#) held around that time, most Filipinos are on board with the new policy. Many genuinely believe that it would [help fight crimes](#) facilitated by mobile phone use. For the telecommunications companies, they, too, [hailed the signing of the law](#), even as they asked for more time to prepare for its implementation.

It is under these circumstances that FMA releases this second briefing paper. It intends to reiterate and highlight the many problems haunting the country's newest identification system. Most of them were anticipated by critics, while a few have ended up surprising people on both sides of the debate. The paper also debunks some of the myths proponents continue to propagate even in the face of clear, contrary evidence.

The hope is that the information in these pages will spark more meaningful discussions about SIM card registration and, if possible, prompt remedial measures from the country's decision-makers and the system's implementing agencies. Such measures should include the possibility of shutting down the system, if circumstances warrant such a drastic step. Something that is not exactly unprecedented. Given the way things are going, so far, that outcome is not easy to dismiss or set aside.

Birth of another ID system

[SIM card registration](#) is a measure that mandates the identification and registration of all SIM card users in a particular jurisdiction. The way it usually works is that upon purchase and before activation of a SIM card, some personal data—which may now include biometric information—of the would-be user is collected and stored by a telecommunications company (“telco”) in a database.

Depending on the approach, telcos may either share the information with government agencies upon demand, or proactively share it (often, with the designated regulator), or they could validate the information against a central government database. For the Philippines, the [bills](#) that eventually led to the current law adopted the first approach. Telcos are required to provide information kept in their respective registries when prompted by at least one of several possible triggers (i.e., upon receipt of a subpoena, court order, or a written request from a law enforcement agency in relation to an ongoing investigation, or if the affected user explicitly consents to the disclosure).

For the lawmakers, the main objective of the system is [to address the proliferation of text-based scams](#). It is supposed to do this by taking away anonymity from the scammers and other criminals responsible for the millions of unsolicited messages being sent to the country's mobile phone user population. On top of that, proponents say the

system also [guarantees a transparent, regulated, and secure mobile environment](#) which, in turn, acts as a stable foundation for a national digital ecosystem.

The law's implementing rules took effect on 27 December 2022. Early estimates for the registration rate were very optimistic. According to one telco executive, simulations they had performed showed that it was technically possible for them to complete the registration of all their 87 million subscribers [in less than 15 days](#). The registration process itself, he said, takes less than five minutes.

Not long into the implementation period, however, it became clear that the system would fall short of people's expectations. The risks its opponents warned about were not unfounded, after all.

Lingering issues

At the moment, there are eight (8) major problem areas that demonstrate how flawed the country's SIM card registration is and how unlikely it is to fulfill its promises.

Low Turnout

The registration process started on 27 December 2022. By 28 January 2023, a month after the online portals opened, 142 million SIM cards remained off the books. That means three months before the deadline set by the National Telecommunications Commission (NTC), only 16% (specifically, 26.64 million) of all mobile numbers had been registered. Smart had only registered 20% of its subscriber base, while Dito and Globe had only signed up 16% and 12% of theirs. At the rate things were going, the NTC said, it was possible that only around 60% of the total number of SIM cards would be registered by April 26. By early March, the Department of Information and Communications Technology (DICT) was already [considering extending](#) the registration period due to low registrant turnout. On April 25, even after several earlier statements [denying the need to extend](#) the April 26 deadline, the government—through the Department of Justice—announced a [90-day extension](#). It was supposedly spurred by the appeal of the telcos, which noted that less than 50% of the country's total active 168 million SIMs had been registered.

“Even before the system’s implementing rules took effect, one telco official already acknowledged that a “big challenge” they were bracing for was how to encourage people to actually register.”

This problem is hardly surprising. Even before the system’s implementing rules took effect, one telco official already acknowledged that [a “big challenge” they were bracing for was how to encourage people to actually register](#). People, he said, naturally hesitate to register given the novelty of the system. With the present state of affairs, this explains why telcos have been trying all sorts of gimmicks and promos to entice people to register. DITO promised its users that they will be rewarded [2GB of mobile data](#) once they accomplish their registration forms. SMART was incentivizing successful registrants with [3GB of mobile data](#). Meanwhile, Globe organized a [National SIM Registration Week](#) in February to encourage their subscribers to register their SIMs. Those who registered that week earned a chance to win tickets to an annual outdoor music and arts festival and a rock concert. As the original April 26 deadline neared and having registered less than half of the total active SIM cards, telcos resorted to desperate means. Globe, in particular, [caused distress to its subscribers](#) when it used the country’s emergency cell broadcast system to push notifications about the deadline. Many questioned the measure since, according to the [Free Mobile Disaster Act](#), such alerts are to be sent out only “in the event of an impending tropical storm, typhoon, tsunami, or other calamities.”

Technical Issues

The rollout of the system was immediately saddled with hiccups, many of them technical in nature. According to the NTC, it received numerous reports of unsuccessful or incomplete registrations, as well as [“down or inaccessible” registration portals](#) that left many subscribers frustrated with the signup process. Apparently, the platforms—despite the telcos’ proclamations—could not accommodate the massive surge in traffic. Other registrants claimed to have not received their one-time PINs, while there were those who encountered a wide array of system errors while navigating the platforms.

Globe was the first provider to temporarily halt its registration process due to technical difficulties. After it registered around 20,000 subscribers, the company made its registration portal temporarily inaccessible. It claimed to have [discovered “potential minor vulnerabilities”](#) that required “careful patching in order to prevent any serious threat to customer data”. It informed the NTC about its decision and [asked for 72 hours](#) to observe its platform.

As far as the other two telcos are concerned, Smart’s registration portal also experienced [heavy traffic during the first day](#) of registration, while Dito—probably because it is the smallest of the three— [seemed to be the only one to escape first-day complications](#). In a statement, Dito claimed that its registration effort was “generally smooth”, allowing it to register a little over 200,000 subscribers during the crucial first day.

At any rate, the NTC became so concerned that it [issued a memorandum](#) directing telcos to report the problems encountered by their respective subscribers during registration. For its part, the DICT [launched a 24/7 complaint center](#) meant to address SIM card registration issues and concerns. The center is under the supervision of the Cybercrime Investigation and Coordinating Center (CICC), which is attached to the agency. By December 29, a mere two days after the start of the registration period, the center reported that it already received [481 complaints](#).

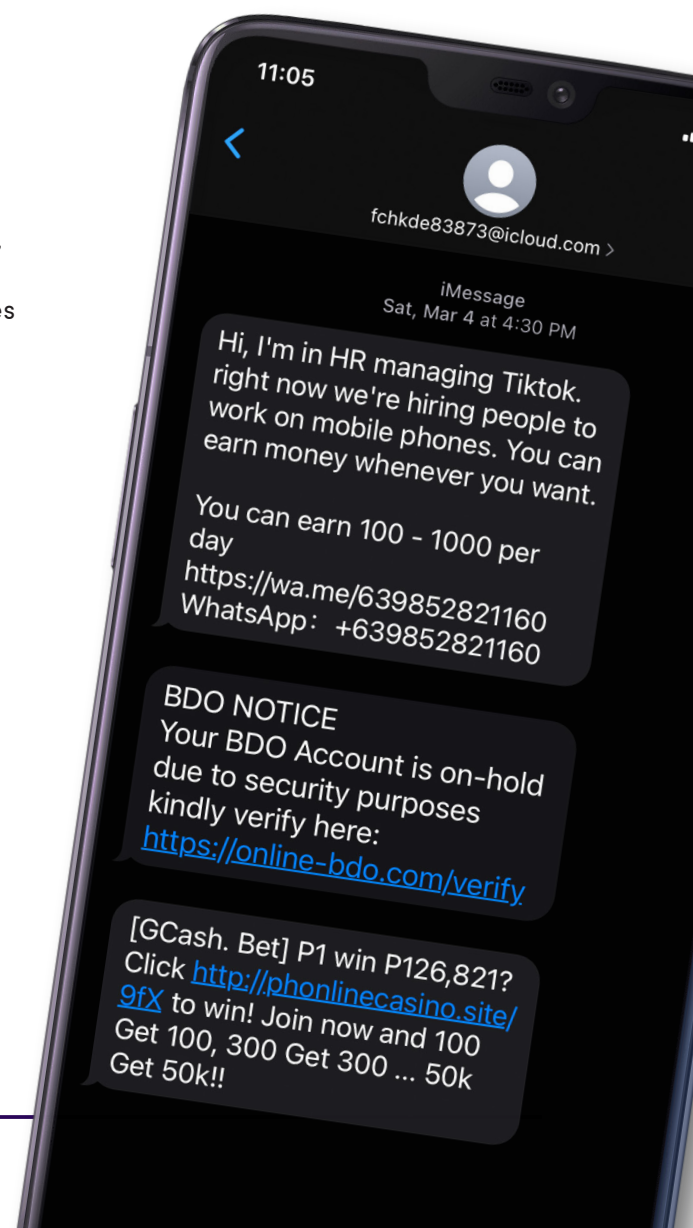


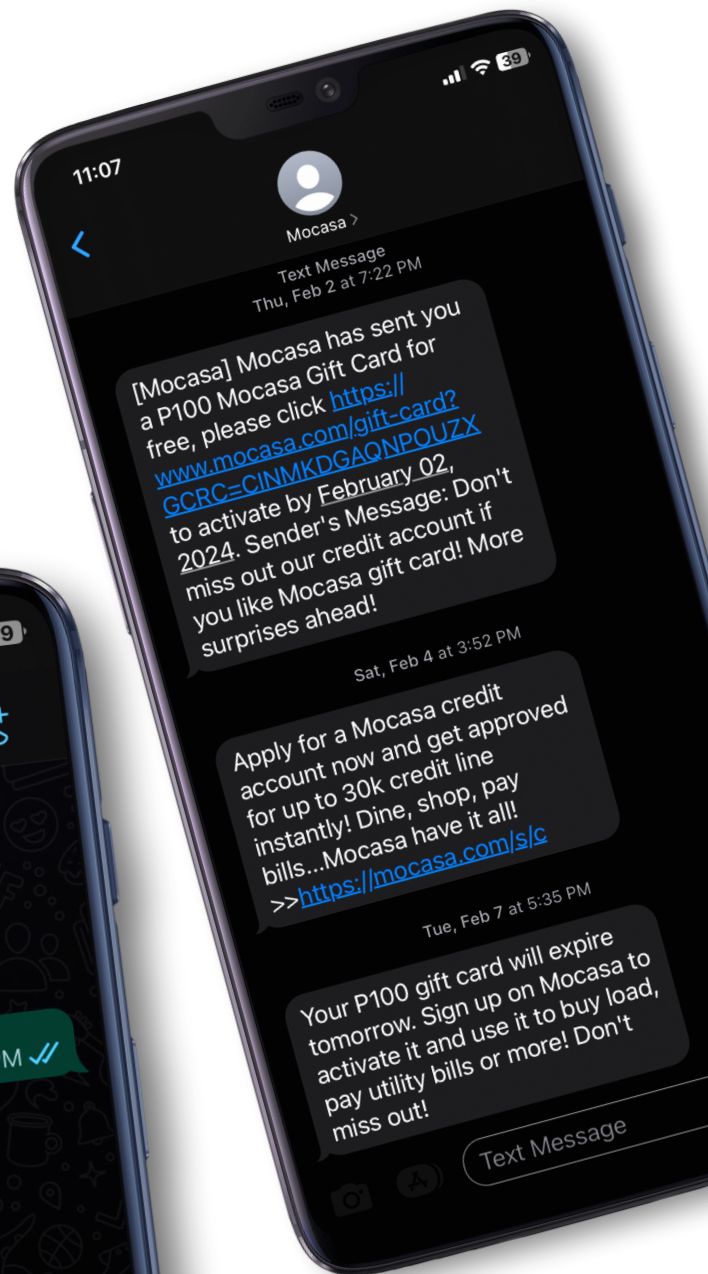
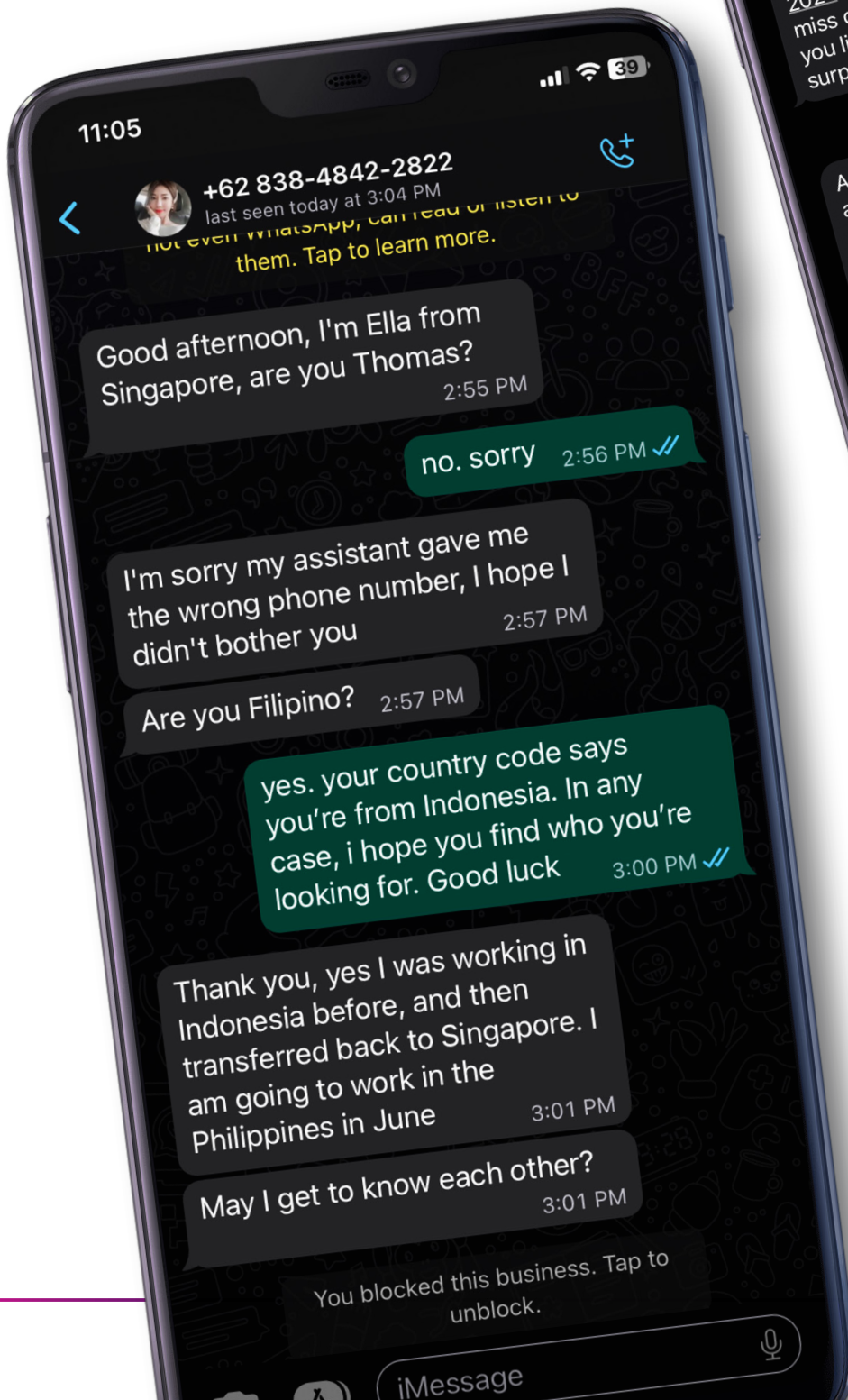
Scams

Once the registration period began, reports surfaced about scammers taking advantage of the situation by offering to assist would-be registrants and asking for the latter's personal details like name, photo, valid ID, birthdate, mobile number, and address. The criminals would publish their offer on social media, sometimes for free, other times for a set fee. Ultimately, there was, of course, no assistance forthcoming, and the perpetrators were simply out to steal people's information (and eventually, their money too).

Globe [warned its subscribers against offers of SIM registration assistance online](#) and advised them not to share their personal data. Customers, they said, should only use the company's official channels.

This problem became so prominent that [the NTC had to come up with a warning](#). It reminded people that the registration process is free of charge, and anyone who claims otherwise is likely engaged in fraud. The agency also warned the public [not to buy pre-registered SIM cards](#) that are being sold in the black market. Meanwhile, the National Privacy Commission (NPC) [also cautioned the public](#) against the spread of emails and text messages containing fake instructions and links on how to register their SIM cards.





Function Creep and Surveillance

Function Creep

The risks posed by SIM card registration come not just from the measure itself but also from the possibility that its corresponding registry will be linked to other ID systems —like the Philippine Identification System (PhilSys), for instance. Many SIM registration proponents expressed their approval of this prospect [even before the system's enabling law was enacted](#).

However, if we look at the experience of other countries in this respect, it's clear that linking identity systems comes with a heavy price. In India, it was revealed in 2017 that a major telco [used its SIM verification process to open bank accounts](#) for its subscribers without their consent. This was done through an e-KYC process that links SIM card verification to Aadhaar, India's controversial national ID system. In Africa, researchers have seen an [“unholy trinity” of digital surveillance](#) in the form of linked digital IDs, mobile SIMs, mobile banking apps, and other digital services. This toxic mix increased the possibility of the SIM card registry and other linked databases [being used to track and target individuals](#), particularly vulnerable groups such as political dissenters, human rights defenders, immigrants, or people living with HIV/AIDS. A distressing thought considering that even the mere possibility of surveillance could send a [chilling effect on fundamental rights like free speech and freedom of association](#).

Now, PhilSys is the national ID system. Established by law in 2018, it has not yet been fully rolled out and its actual use has been minimal so far. Despite this, it already stores the personal information of millions of Filipinos. The possibility that the government will find a way to connect it to the SIM card registration system is high, if not a foregone conclusion. Telcos are among the foremost supporters of this prospect. As soon as RA 11934 was passed, they immediately aired their additional “wishes”, including having interconnected ID systems. Globe maintained that it had always believed that the success of SIM card registration relies heavily on having [a national ID system](#). For DITO, it hoped that both the national ID system and the passport system will be used as validation tools for SIM card registration. This would let telcos [avoid establishing another database](#), which can be time-consuming and resource-heavy.

But there is more to function creep than just interconnected ID systems. There is also the likelihood that telcos will utilize the

new database under their stewardship for their own purposes. The first example was evident as early as the launch of the registration system.

Back then, controversy arose almost immediately after people complained of tick boxes put up by some telcos asking for their consent to the use of their personal data for marketing and profiling purposes, as well as the sharing of their personal data with third-parties. This led to the NPC [meeting with the telcos](#) to address the public's data privacy concerns. In the case of Globe, registrants were asked if they would like to [“receive commercial and promotional alerts, personalized advertisements, financial service offers, surveys, and similar communications](#) via SMS, email, in-app notifications and other means”. With Smart, subscribers had the option to agree to [“receive customized offers, recommendations, and promotions”](#) through their contact details, using different channels such as SMS, voice calls, and emails. If they agree, subscribers admit to recognizing the need by Smart to analyze their usage information in order to create their personal profile. Both companies have insisted that there is nothing wrong with their activities since agreeing to the additional uses is only optional.

The inclusion of selfie verification as part of the registration process was also immediately [identified as problematic](#), particularly since it is an additional data collection that is not sanctioned by the law or its implementing rules. As of this writing, however, this mechanism remains suspended after causing technical issues during the registration process.

Surveillance

As most critics are quick to note, it is not inconceivable [that the SIM card registration system will be “weaponized”](#) and used as a tool of “mass surveillance and authoritarianism”. The Philippine government, they point out, is [notorious for unlawful surveillance activities and data privacy violations](#). It has, for instance, experienced a number of high-profile surveillance controversies in the past, which remain unresolved to this day.

Also alarming is the fact that in expressing support for the measure, the Philippine National Policy (PNP) has not guaranteed that the SIM registry will only be used to investigate cases of spam and text scams or other SIM card-aided crimes. Instead, they simply claim that it will be [useful as a crime deterrent](#) and when tracking criminals, in general.

“Is the government ready to punish them further by deactivating their cellular phones and services to deprive them of their livelihood and their inexpensive yet efficient means of transportation and communication?”

These fears are not unique to the Philippines. In Kenya, SIM registration involves providing biometric data, including facial images. According to at least one broadsheet, what is most concerning about the system is how the confidentiality of the registration information or the right to privacy of the registered users will be maintained. That the law allows any “competent authority” with subpoena power to compel a telco to disclose personal data makes the system vulnerable to certain government entities. They, too, are afraid that the law could be weaponized, in that it could be used to surveil and target perceived enemies of the State, including journalists, activists, critics, and human rights defenders.

Exclusion

Like any ID mechanism, a SIM card registration system has that inherent potential to exclude, and, more often than not, it usually impacts people that are already disadvantaged.

People saw this Nigeria where, earlier this year, a third of all mobile users—many of them women—were barred from making outgoing calls after failing to register with the national ID database. The country’s ID system rolled out almost ten years ago, but it was only in 2020 that the telecommunications regulator required all active phone numbers to be linked to the registered ID of their users. Millions were unable to register their SIM cards due to privacy concerns and other challenges such as logistics (e.g., physically traveling to registration centers) and lack of valid IDs (e.g., not being registered in the national ID system). The disenfranchised women came mostly from rural areas where they already deal with patchy mobile networks, poorly built roads, and sometimes the lack of means to travel to the designated registration centers.

In Kenya, a similar SIM card registration directive was issued in February 2022. According to reports, less than 12 hours before the extended deadline, over 10 million subscribers still had not registered and were in danger of being disconnected. The regulator stood firm on its imposed deadline, completely oblivious, it seemed, to the plight of those who are unable to register due to various valid reasons. It noted that, anyway, deactivated mobile users can still register and/or re-activate their SIM cards even after the deadline elapses.



Things are no different here in the Philippines, with at least one study already expecting [a segment of the country's subscriber base to be disenfranchised](#) (i.e., those without valid IDs and/or access to registration portals). This gives credence to the Philippine Chamber of Telecommunication Operators' (PCTO's) [original claim](#) that a mandatory SIM card registration system will strip Filipinos of their right to communicate.

The government is supposed to be aware of this and even has the numbers to prove it. According to one DICT executive, geographically isolated and disadvantaged areas represent [around a third \(27%\) of the total number of barangays across the country](#). This is why, she says, the agency is collaborating with telcos and other government offices to facilitate registration even in these regions. Take the case of the NTC which, in January this year, talked about [the government's plans to ensure SIM card registration in 15 identified remote areas](#). In the chosen locations, they established free WiFi sites for assisted registration purposes. The Department of Justice, meanwhile, would set up one-stop-shops where subscribers can get NBI clearances they can then use as IDs when registering their SIM cards.

Telcos have long known about this, too. Back in 2013, the PCTO submitted a position paper to Congress opposing SIM card registration on several grounds, including potential disenfranchisement. They highlighted, in particular, those subscribers from rural areas who would have difficulty traveling to urban centers for the registration process and poor subscribers who could hardly afford loading their prepaid SIMs. Regarding this particular demographic, the group asked if the government was ready to punish them further by deactivating their cellular phones and services to deprive them of their livelihood and their inexpensive yet efficient means of transportation and communication.

Today, telcos appear to have made peace with that outcome given their full support for the system. They seem content with just ramping up their assisted registration initiatives. [Globe, for instance, partnered with a leading supermarket chain](#) to hold assisted registration in some of the latter's branches. It was part of its effort to help its users, especially senior citizens, Persons with Disabilities (PWDs), and those who don't own smartphones.

It also offered assisted registration services during popular regional festivals like Sinulog in Cebu and Dinagyang in Iloilo. [Smart has also partnered with SM Store and SM Supermalls](#) to make its registration process more accessible to the public. The telco has also [deployed assisted registration booths in a number of far-flung municipalities](#) in collaboration with regulators and the local government units themselves.

Despite these efforts, however, there remains no credible solution to the problem that a significant portion of the population do not have IDs or even civil registration papers needed for registration. According to the Philippine Statistics Authority, as of 2021, there were a total of [9.26 million Filipinos](#) who still do not have birth certificates. For them, it is extremely difficult to apply for government-issued IDs.

Effectiveness

When the barrage of spam and phishing text messages somewhat peaked in early 2022, so too did calls for the passage of the law—even from sectors previously opposed to it or wary of its risks. Nearly all of them described the measure as a much-awaited solution to recurring problems. They emphasized its urgency, as well as the expected value of its impact. This, despite not offering an iota of proof that it would be as effective as they made it out to be.

The failure to provide evidence does not appear to be an oversight or mere coincidence. After all, as of this writing, there remains no concrete proof from anywhere in the world that directly links mandatory SIM card registration to crime prevention. Meanwhile, there are plenty of accounts showing how easy it is for criminals to circumvent such a system via a wide array of tactics.

As such, it becomes easy to see the flawed logic of local SIM card registration proponents when they advocate for the merits of the measure.

Take, for instance, law enforcement agencies and even telcos, both of whom suggested possible explanations for scammers' access to mobile users' personal data. According to the Philippine National Police (PNP), [personal data may have been sold and bought in the dark web](#) where parties to transactions could remain anonymous and untraceable. If they are right, though, what makes them think the same would not happen when it comes to perpetrators of spam and phishing activities?

For major telco, Smart, it offered a theory positing that [foreign actors working with domestic operators are the likely culprits](#) behind spam and scam messages. If that were true, that means SIM card registration would only address that part of the problem attributable to entities based in the country. It leaves the overseas component intact and free to operate.

One case that is frequently brought up when there is talk of the effectiveness (or lack thereof) of mandatory SIM card registration is that of Mexico. In 2009, the country introduced the National Mobile Telephone User Registry scheme. It repealed the law in 2012 after a policy assessment showed that it had failed to prevent crime the way it was supposed to. Nine years later, in 2021, the government reintroduced the registration scheme. This time, requiring the submission even of biometric data, supposedly to counter the threat of extortion. When the law was challenged in court by several organizations, including the telecommunications regulator, it was declared unconstitutional by the Supreme Court, which said the registry would violate human rights and that the need for data in limited circumstances (i.e., to prevent certain crimes) fails to justify infringement on the right to privacy.

Back here in the Philippines, criminals have already begun deploying new strategies designed to beat the registration system. This early, spam and scam messages shared via SIM cards bought abroad or using other online delivery methods (with messages showing email addresses as sources instead of mobile numbers) are already starting to pop up. There is also a burgeoning trade involving pre-registered SIM cards (i.e., using fake or stolen identities) as evidenced by [at least two police sting operations](#) that managed to snag the sellers, along with their contraband.

Anonymity

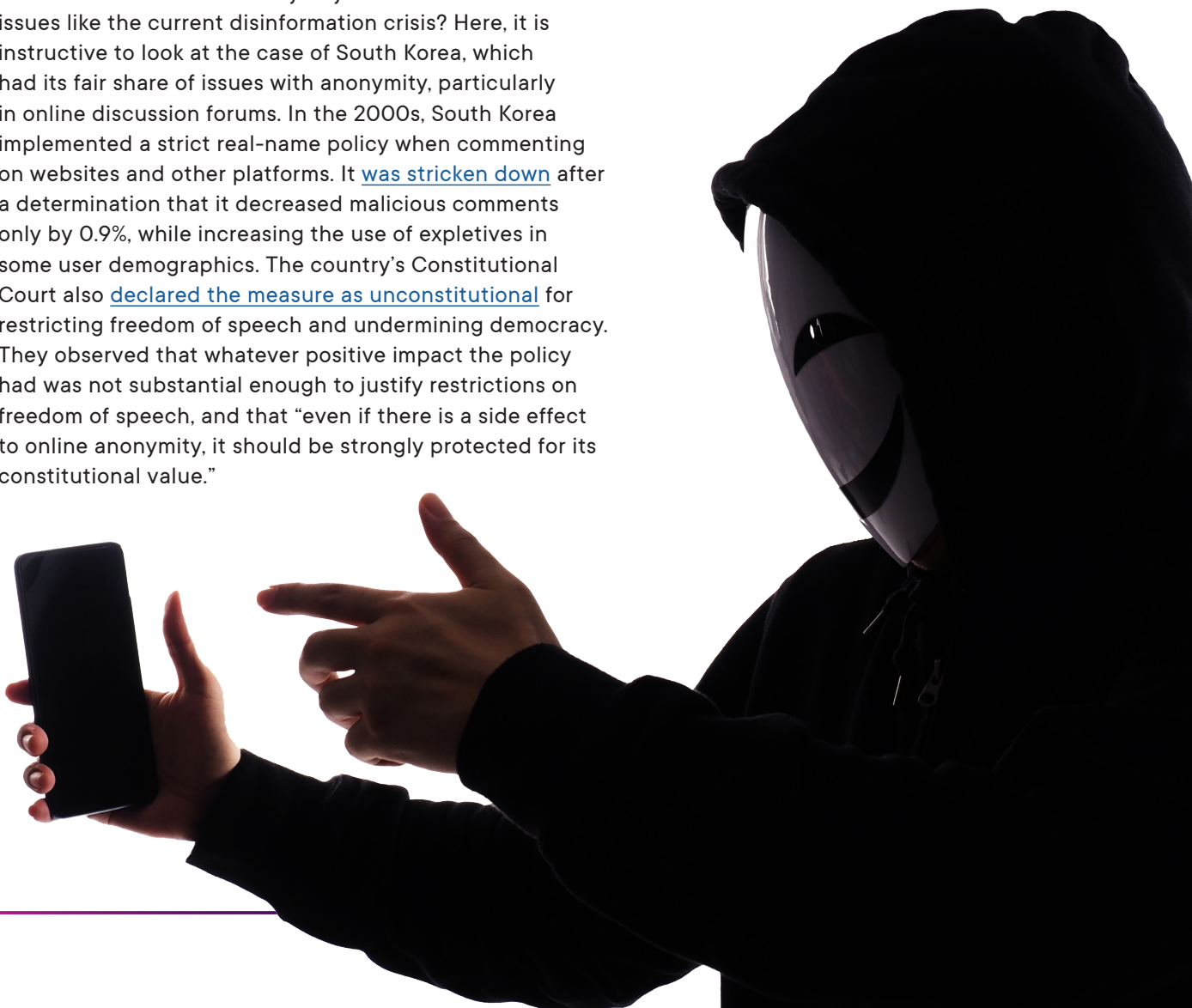
The push for SIM card registration forms part of a broader movement to erode or at least discourage anonymity while using information and communications technologies. Once it's in place, the potential for anonymity of communications is effectively taken away, along with associated rights like freedom of expression and freedom of association. Location-tracking and communications surveillance (or interception) become easier to carry out.

In the case of the Philippines, anonymity has not exactly endeared itself to the population, given the many ways it is linked to unlawful or at least inappropriate behavior. For instance,

whenever the problem of disinformation is brought up, putting the blame on anonymity is never far behind, thanks to the faceless individuals acting as very effective vectors of false, harmful information. During the Duterte administration (2016–2022) and leading up to the May 2022 elections, the anonymity debate became a major talking point for this very reason. It came as no surprise then that SIM card registration (along with social media account registration) was proposed as a plausible [solution to information disorder](#).

Consistently absent in most discussions, though, are the crucial benefits anonymity also affords, particularly to marginalized groups and those with serious concerns about their safety. What becomes of their fate is rarely taken up.

Another question that also needs serious thought is whether the erosion of anonymity would even solve issues like the current disinformation crisis? Here, it is instructive to look at the case of South Korea, which had its fair share of issues with anonymity, particularly in online discussion forums. In the 2000s, South Korea implemented a strict real-name policy when commenting on websites and other platforms. It [was stricken down](#) after a determination that it decreased malicious comments only by 0.9%, while increasing the use of expletives in some user demographics. The country's Constitutional Court also [declared the measure as unconstitutional](#) for restricting freedom of speech and undermining democracy. They observed that whatever positive impact the policy had was not substantial enough to justify restrictions on freedom of speech, and that “even if there is a side effect to online anonymity, it should be strongly protected for its constitutional value.”

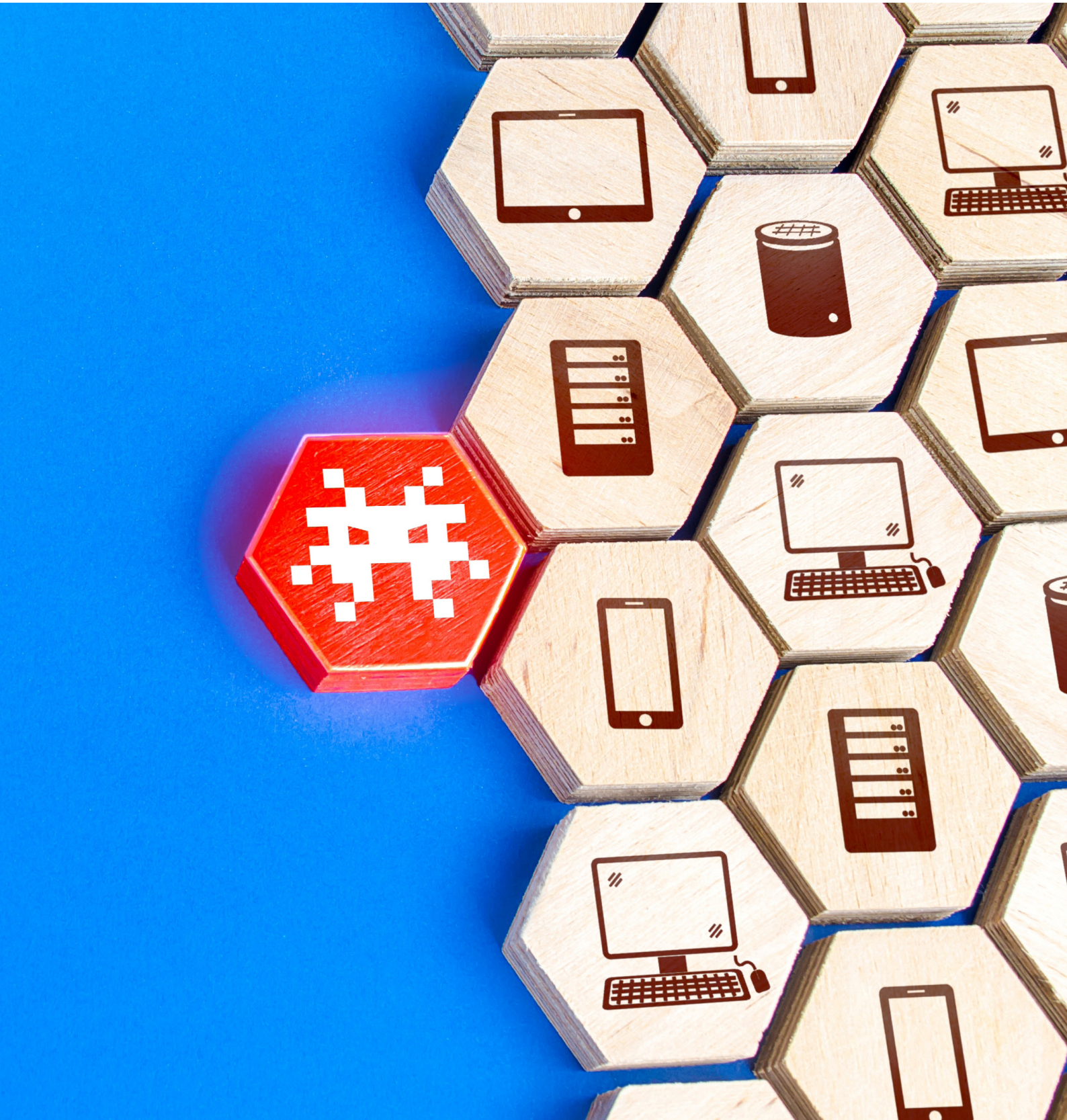


Security Risk

While the three databases created by mandatory SIM card registration are supposed to establish a more secure digital ecosystem by deterring crimes, or at least making their resolution easier, they inevitably become security liabilities, too. After all, centralized databases are widely known to be honeypots that attract a lot of unwanted attention from bad actors. Telcos, in particular, are vulnerable. In 2021, several analytics companies reported that the telecommunications industry is the most valuable target for cyber criminals, making them prime targets of cyber attacks. Most databases accessed through these types of attacks contain client data that are eventually used to target spam messages, scams, and phishing.

For concrete examples, one need not look far. In August 2022, the government-owned telecoms firm, PT Telkom Indonesia, experienced a data breach, along with another government entity. Later in the same month, another massive data breach was reported. This time, it involved data from 1.3 billion SIM card registration records. The 87 gigabytes worth of leaked data supposedly included each Indonesian's national ID number, phone number, telco provider, and SIM card registration date. It was being offered in an online hacker marketplace for US\$50,000. The same hacker posted more leaked personal information, including that of Indonesia's Communication and Information Technology Minister, to expose the government's poor data protection practices. Meanwhile, the following month, Australia's second largest telco also suffered a major data breach as a result of a cyber attack.

In Philippine shores, some of SIM card registration's sponsors in Congress seem wary of the risks posed by this system they helped create. After the law was enacted, one said the DICT and the NTC should be "extremely careful" in the handling of personal data of the country's mobile phone users. The agencies were told not to rush its implementation and make sure first the system is "future-proofed" against data breaches and other security risks. It is worth noting, though, that no concrete steps were given in terms of making sure the system is better protected.



Other observations

With so many issues now hounding the system, the uncertainty that revolves around it has only increased with time. This helps explain why supporters have started to temper people's expectations. In stark contrast to the strong narratives and arguments raised in favor of SIM card registration back when it was still being proposed, statements from the implementing agencies have now shifted to a more tamed tone. When one now listens to NTC Officer-in-Charge, Ella Blanca Lopez, one is told that the measure is [not an "end-all solution" to cybercrimes](#), after all.

Meanwhile, opposition groups continue to grow in numbers and voice out their concerns, especially after many of their earlier predictions have already been confirmed.

For advocacy group, Digital Pinoys, they believe the law is [unlikely to eliminate SMS spam and may even make it worse](#), should registration data be compromised. The Junk SIM Registration Network, on the other hand, continues to highlight the [risks posed by a centralized database](#) by pointing to the experience of other countries. It also [reiterates its concerns over the ID requirement](#), and its ability to disenfranchise marginalized sectors. For Karapatan, a human rights organization, the law could [lead to more security breaches and privacy intrusions](#). Meanwhile, [Citizenwatch Philippines](#) has raised the practical concern of registering over 100 million SIM cards within the prescribed period. According to the group, the implementation strategy needs to be as painless and non-disruptive as possible, with people being given clear registration instructions. A credible but secure identification verification process is going to be crucial, they said. They also warn of the danger enormous databases will create, especially if they are compromised and fall into the wrong hands.

Amid all these adversities, government regulators have so far revealed themselves to be unprepared, ill-equipped, and weak-willed. Typical characteristics, some would say, of Philippine government bureaucracy. For example, when it came to addressing allegations that telcos were engaging in function creep (by adding tick boxes in their registration forms), a feeble NPC responded by simply directing the companies [to separate the notices and tickboxes unrelated to](#)

[SIM card registration](#). It was as if the only thing worrisome about the setup was [the misconception or confusion it could create](#). Nevermind the fact that the telcos were getting a free ride on the SIM card registration train and turning the database into a potential data resource for their own business interests. On the other hand, agencies like the NTC and the DICT have not shown anything to suggest that they have already settled crucial issues like the lack of IDs of would-be registrants and the proliferation of pre-registered SIM cards.



“Amid all these adversities, government regulators have so far revealed themselves to be unprepared, ill-equipped, and weak-willed. Typical characteristics, some would say, of Philippine government bureaucracy.”



Conclusion

When one is confronted by the prospect of a failed initiative, it is a valid recourse to explore alternative measures or solutions. The current status of the SIM card registration system suggests that the government should already be exerting efforts towards that end.

In previous Congresses, the establishment of a “no call, no text, no email” registry has been repeatedly proposed as some form of spam protection. It involves setting up a [non-mandatory registration system](#) for subscribers who do not want to receive promotional messages. Another policy proposition has been to explicitly prohibit telcos or content providers from sending unsolicited messages intended as commercial or promotional advertisements. Subscribers must opt in to receive such messages and should also be allowed to [opt out](#).

In the meantime, the responsibility of the NTC, the NPC, and other regulators to protect the people and their personal data, as well as to holding telcos and other stakeholders (including fellow government agencies) to account is going to be critical. The Philippines is supposed to consider itself lucky because unlike some countries with similar registration schemes, it actually has a data protection law and a data protection authority to turn to. It cannot, though, as the NPC has been subpar so far in its posturing and in its response to challenges. By this time, its active support for and promotion of the measure is already [well documented](#). Instead of being a neutral regulator, it has adopted a position, one that even conflicts with its earlier admission about the system bringing out [higher risks of personal data breaches](#). Also, for all its bluster claiming that data protection is one of the cornerstones of a successful SIM card registration system, the Commission has not shown anything to substantiate this point. On the few chances it’s been given to prove its resolve, it has shown its willingness to look the other way and give

telcos a free hand. That's quite a letdown coming from the country's privacy watchdog. It needs to step up in a big way if it is to earn back that title. This is also true for the other regulators who also need to live up to their respective mandates.

At this time, a petition to issue a temporary restraining order (TRO) and declare the SIM Registration Act as unconstitutional has been filed before the Supreme Court, but the TRO request was denied on the same day the 90-day extension was announced. It remains to be seen how the Supreme Court will rule on the constitutionality of the law, which is being assailed on the grounds of violation of free speech, the right against unreasonable searches and seizures, and privacy of communications, among other rights.

It's already been days since the original registration period expired and was extended for an additional ninety (90) days. At the time of the original deadline, only less than 50% of active SIM cards in the country had been registered. The figure will, of course, increase as more people are convinced (or coerced) by the government and the telcos. But then so too will many questions arise and persist, if most of the problems cited here remain unresolved.

In terms of inclusion, how many people will end up losing access to mobile services because they continue to have no government-issued IDs? With data quality, how reliable are the telcos' registration records, in view of the proven ability of bad actors to register SIM cards under false or stolen identities? On security, what assurances does the public have that the SIM registries will not be compromised, similar to what happened in other countries like Indonesia and Australia? And regarding effectiveness, do the government and telcos have any answer to spam and scam messages originating from sources that fall outside the scope of the registration system?

If questions and concerns like these are not addressed, not only will SIM card registration fail spectacularly in delivering on its promises, it will also cause problems far worse than that it is meant to solve. Critics and rights advocates have made this very clear right from the beginning. What's changed is that there are now obvious signs available for everyone to see. People are beginning to realize just how much of this ID system was built on nothing but a molehill of unsubstantiated claims and lofty promises. Once those claims and promises crumble and dissipate into empty space, so too will this system falter and maybe even meet its early demise.



The Foundation for Media Alternatives (FMA) is a non-profit service institution whose mission is to assist citizens and communities—especially civil society organizations (CSOs) and other development stakeholders—in their strategic and appropriate use of the various information and communications media for democratization and popular empowerment.

Since its formation in 1987, FMA has sought to enhance the popularization and social marketing of development-oriented issues and campaigns through media-related interventions, social communication projects and cultural work. In 1996, FMA streamlined its programs and services in both traditional and new media, with a major focus on information and communications technologies (ICTs), to enable communities to assert their communication rights and defend their rights to information and access to knowledge, towards progressive social transformation.



(632) 7 356 7965



info@fma.ph



29-P Matimtiman Street

UP Teacher's Village

Quezon City