Foundation for Media Alternatives

vol. 01

EXPOSÉ

EXPOSÉ

Data Rights in the time of COVID-19

CONTENTS

FOUNDATION FOR MEDIA ALTERNATIVES

2021

Published by the Foundation for Media Alternatives

Unit 203 CRM Building III, No. 106 Kamias Road
East Kamias, Quezon City
T. (632) 7753 5584
E. info@fma.ph

Photos by:

Jamael Jacob
Amina Filkins, Anna Shvets, August de Richelieu, Brayan Vieira, Budgeron Bach, Burst, Cottonbro, Cristian Dina, Denise Duplinski, Engin Akyurt, Ingo Joseph, Julia M Cameron, Karolina Grabowska, Ketut Subiyanto, Klaus Nielsen, Korhan Erdol, Krisia Vinzon, Mart Production, Mati Mango, Mikhail Nilov, Oleg Magni, Photomix Company, Pixabay, Samson Katt, Sebastiaan Stam, Slondotpics, Thirdman, Thisisengineering, Two Dreamers, Tyler Lastovich, and Vanessa Garcia from *Pexels*

Layout by C Jean Regala

EDITOR'S NOTE

EXPOSÉ is an online publication of the Foundation for Media Alternatives (FMA) that aims to take on current privacy and data protection issues and events in the Philippine context. In this maiden issue, privacy and data protection issues surfaced or highlighted by the ongoing COVID-19 pandemic take center stage.

In the succeeding pages, FMA staff and fellow privacy advocates take their picks among the litter of privacy-related controversies this past year and unpack them in a series of information-rich but bite-sized articles. They correctly note that most of the problems have been around even before the onset of this global public health crisis. If anything, the pandemic has only served to make them more prominent—and worse, in many instances.

A comprehensive understanding of these issues is the necessary first step towards crafting appropriate responses and solutions. Incidentally, that is also the very foundation upon which EXPOSÉ, as a communication tool, stands and obtains its reason for being.

Read along and don't forget to share.

Data Privacy for the Departed

Jam Jacob

Life's fleeting nature has been on people's minds lately, thanks to the scourge that is this COVID-19 pandemic. For the privacy-conscious, what usually comes up are related but more specific questions like: do those who have passed away still get to enjoy privacy? It's a discussion that has surfaced a number of times this past year, not necessarily due to the health crisis but because of events that have transpired in the midst of it.

One of them took place in March 2020, back when the pandemic was still in its early stages, at least here in the Philippines. An aircraft being used as an air ambulance burst into flames and exploded while taking off, killing all passengers on board. Word got out and spread quickly that in about an hour, the names of those who perished were already all over social media.

No less than a copy of the General Declaration (and Air Cargo Manifest) for the flight—which did not only identify the victims, but also gave away other details like their sex, birthdate, and passport number—was being shared across the major social media platforms. Media organizations were in on it too, as some included the same document in their respective news reports.

There were people who questioned the propriety of having all that information leaked to the public. It was possible that relatives of the victims had not yet been notified by authorities of the tragedy. They must have been so distraught to learn about it from other people, especially from complete strangers.

A few months later, the same issue was brought to the spotlight by another controversy.

It was July and reports from anonymous sources had suggested the presence of COVID-19 cases within the country's prison system, including some that resulted in the deaths of well-known inmates. When pressed for comment, the Bureau of Corrections (BuCor) admitted the rumors but refused to disclose the identities of the deceased, citing the provisions of the country's data protection law: the Data Privacy Act of 2012 (DPA).

The BuCor surprised many with its position. It stood in contrast to the issue of the leaked plane manifest where it was likely that government personnel were behind the public disclosure of the sensitive data. The Department of Justice eventually resolved the issue when it announced the names of the affected prisoners, but not before various parties had already managed to voice out their opinion on the subject.

Take the case of Senator Franklin Dwrilon who disagreed with BuCor and pointed out that the state policy behind the DPA is "to protect people from being harmed from the invasion of their property". A person's death, he said, is not among those information whose disclosure is prohibited by the law. He also emphasized that prisoners have a limited right to privacy, given the suspension of some of their civil and political rights while incarcerated.

Meanwhile, his colleague at the Senate, Senator Panfilo Lacson, sided with the agency and said that the DPA may apply to prisoners especially if their deaths are caused by a dreaded disease that could subject their immediate family to "undue discrimination" and stigmatization.

The National Privacy Commission (NPC) weighed in on the matter, too. It held that the DPA does not apply to information about public figures like high-profile inmates. Thus, the law cannot be used to withhold such data even when they concern sensitive personal information.

Curiously, though, none of those who had spoken out thought of bringing up the fact that the individuals whose rights were being debated on were already deceased.

Nevertheless, both cases still raised the same set of questions that other observers were already taking up in the sidelines: is the disclosure of personal data about a deceased person legal? Or does it amount to a violation of the DPA? Do the dead still enjoy any protection offered by the law?

Rights: They're Alive!

If one looks at the DPA, the answers to all those queries would seem to be in the affirmative.

According to the law, the heirs of a man may invoke his rights as a data subject at any time after his death. And so, in the same way that that man could challenge the lawfulness of the disclosure of his personal data (and even file a related complaint) while he's still alive, so too could his relatives after his death.

For many, this notion that a lifeless body could somehow still assert some rights—even if it's to be channeled via living individuals—is rather special or at least uncommon. That is not to say though that it is unique or unprecedented.

Under Philippine law, an individual's juridical personality is generally extinguished once he or she dies. That's supposed to mean he or she will retain no legal rights. Exceptions do exist, though, such that some rights (and even obligations) may be transmitted by a person to his or her heirs via different means (e.g., law, contract, will, etc.). For example, by law, people get to distribute their properties among their heirs after they're gone. Similarly, according to the country's libel law, it is possible to prosecute someone who "blackens the memory of one who is dead".

Accordingly, it would be accurate to say that people get to keep some rights even after death. What the DPA does is simply add a few more to that existing set of rights.

In other countries or territories, it appears to be a matter of culture or preference. Some are equally generous when affording people rights post mortem. Others are not.

The European Union's General Data Protection Regulation is a case in point. Widely considered to be the benchmark for all modern data protection laws, it categorically says it does not apply to the personal data of deceased persons. Despite this, though, it has not shut the door completely to the idea. This is because it specifically says that member States can provide for rules regarding the processing of personal data of the dead.

Today, some European countries that are part of the Union do recognize data protection rights favoring the deceased.

In France, since 2016, individuals can regulate the processing of their personal data after their death. Under the French Data Protection Act, a person can give data controllers either generic or specific instructions as regards the retention, erasure, and communication of their personal data once he or she dies. Designating a person who will make sure his or her instructions are followed is also allowed.

Meanwhile, a 2018 amendment to Italy's Data Protection Code declares that the rights of a deceased data subject may be exercised by any person who: (1) has a personal interest; (2) is acting in the interest of the data subject as an authorized representative; or (3) is acting for family reasons "worthy of protection".

This trend is not limited to legislation either. In July 2018, for instance, the German Federal Court of Justice held that the heirs of the deceased have the right to access the Facebook account of their dead relatives, premised on the idea that a social media profile is inheritable just like physical goods.

"...the heirs of the deceased have the right to access the Facebook account of their dead relatives, premised on the idea that a social media profile is inheritable just like physical goods."

Whether or not the Philippine Supreme Court will follow suit is still something to watch for. It seems the high court has yet to come across a case that would allow it to discuss its views on the matter.

There are those who argue that the Zarate v. Aquino III (2015) case would have been a good opportunity for the Court to declare its theory. Unfortunately, just like Vivares v. St. Theresa's College (2014), which the Court took on first, it involved a habeas data petition wherein the petitioners did not make any effort to cite or invoke the provisions of the DPA. In Zarate, the Supreme Court ruled that heirs of a deceased cannot join a habeas data petition because the Rules on Habeas Data contemplate a petitioner or aggrieved party who is still alive. Accordingly, heirs have no legal standing to sue on behalf of their deceased relative.

As far as NPC official opinions are concerned, it's interesting to note that, beyond its remarks regarding the deceased inmates fiasco, it has already confronted specific questions that involved the personal data of the departed. Unfortunately, its answers either steered clear of any discussion or did not have to resort to one in order to address the main query. Its AdOp 2018-035 simply declared that the submission of personal data of deceased persons is allowed when required by law, while in AdOp 2020-004, it held that the processing of personal data of barangay officials, including any related claimed death benefits, fall outside the scope of the DPA.

The ball then, as they say, is still very much in play.

The most recent incident to unearth this subject concerned the death of flight attendant, Christine Dacera, which made sure to cast a gloomy start to 2021. Within hours of the earliest accounts of her death, social media and news headlines were already awash with rumors and conspiracy theories trying to explain the circumstances surrounding her demise.

Just like in the case of the plane victims, official documents featuring sensitive details pertaining to Dacera (or her body) ended up anew in the public domain. The difference this time was that the harm caused by the exposure did not only affect Dacera and her family, but more so, those accused of having had a hand in her death.

Early conclusions derived from the leak strongly suggested that she was drugged and raped first before she ended up dead. This resulted in massive public outrage against the suspects. The police made it exponentially worse by prematurely releasing their names and declaring the matter as "case closed" despite having very little evidence on their hands.

Future Day of Reckoning

If anything, the stories cited here point to the continuing importance of proper personal data processing, even after the person involved is already gone. This, since not only does such person still retain rights as a data subject, but also because any harm or damage resulting from the inappropriate use of his or her personal data could also affect other people.

Any prudent organization ought to keep these two points in mind.

Ultimately, that the application of the law won't be simple and will probably be subjected to legal challenges is almost certainly a given. Its language definitely doesn't make it easy for anyone (including the courts) to interpret its full meaning and facilitate its proper implementation.

There are also plenty of questions that still remain unanswered: who among one's heirs can exercise one's rights as a data subject? Is there an order of preference that will be followed? If there is none, what happens if one or more heirs want to exercise the rights? And what if they disagree as to how the rights will be exercised? Also, is it possible for a person to authorize someone who is not a legal heir to later exercise his or her rights after his or her passing?

These concerns and more will be resolved in due time. It's just a question of when exactly.

To the more discerning data controllers, that shouldn't matter much. What's important is that they avoid any transgression of the DPA that is inadvertent or brought to bear by sheer ignorance. While there has been no known attempt by an heir to date that seeks to enforce or assert the rights of a deceased loved one, data controllers should still be prepared to recognize one, just in case an individual does come along and tests the teeth of the law.

For data subjects, there is at least comfort in knowing that in the event of our departure from this world, we are not completely deprived of our rights and other protections we are currently afforded by the law.

NOTE: An abbreviated version of this article first appeared in GMA News Online on 22 March 2021.

Online Outbreak

Maris Miranda

Every now and then, I would receive unsolicited messages on my phone that usually offer personal loans or obscure condominium ads. Most of the time, they are harmless and only pose as a minor nuisance. I try my best to ignore them, and often delete them instantly. I wish I could say the same when it comes to emails I get from banks. Whenever they're involved, I can't help but feel paranoid. Every time I receive one, I check every detail of the email, grammar and spelling included.

The reason is quite simple. By now, I've heard so many stories of people getting phishing emails that really look legitimate. In many cases, the sender feigns concern for the recipient and the latter's account. It warns of potential problems with the said account and uses this to ask the recipient to update his or her credentials. All the while, the real objective is to get the recipient to disclose his or her log-in information on a fake bank website, where they are collected and later used to steal money or at least compromise the affected account.

Just the thought of that happening to me gives me plenty of grief! And to think that's only one online threat out of many.

Unfortunately, living with all these dangers in cyberspace is inevitable. It's nearly impossible for us to live our lives today without resorting to the internet. This COVID-19 pandemic has made this abundantly clear. Very few would be able to say they could have made it this far without turning to the web at least once.

For online criminals, the health crisis has been a boon. Instead of sympathyzing with the rest of society, they have treated the pandemic as just another chance to ply their wares. They've taken advantage of the instability and have caught many individuals and organizations unprepared for the increased scale and sophistication of modern-day crimes. Most vulnerable have been neophyte internet users who know very little about cyber hygiene and data protection measures.

Indeed, according to the International Criminal Police Organization (INTERPOL), there has been a significant spike in the prevalence of spam messages, malware incidents, and malicious COVID-19-related websites. Here in the Philippines, a recent survey showed that cybercrime increased by 19% in 2020, ranking fifth among the economic crimes experienced by companies.

Hack and Phish

Two of the more common types of cybercrimes currently surging are hacking and phishing. In 2020, they were the top causes of data breaches in most regions. They are alike in that they can both allow malicious actors to unlawfully obtain personal data, often for personal reasons or financial gain. Perpetrators could be anyone around the victim: former employees, professional criminals, state actors, or even complete strangers just looking for computers to access as a prank. Certainly, part of the blame sometimes goes to the victims too. Since many people are still unfamiliar with digital platforms and devices, they easily fall prey to all sorts of online trickery.

Phishing involves a malicious actor pretending to be a legitimate entity that persuades the target to disclose sensitive or classified data. According to one security firm, roughly 91% of all information security breaches starts with some form of phishing scheme. During this pandemic, INTERPOL estimates that around 59% of cyberthreats recorded have involved phishing, scams, or fraud. In Southeast Asia, phishing attempts during the first half of 2020 already saw a 39% increase compared to the previous year, mostly targeting small and medium enterprises. Historically, people are more susceptible to social engineering attacks during turbulent times, since they tend to seek information wherever they can get it during these periods. Chinese and Russian hackers reportedly use this strategy frequently on their targets, including the Philippines.

Here in the country, phishing supposedly increased by more than 200% during the first half of 2020, enough to make it the country's top cybercrime. One major commercial bank claims having taken down around 2,000 phishing sites preying on donors in just six (6) months.

Hacking, on the other hand, involves a malicious actor that breaks into a computer system either through direct access, or indirectly through phishing, theft of login credentials, or malware. A Philippine university student portal, for instance, was breached in June 2020 after many members of the school community were tricked into clicking pharming links sent by unidentified individuals.

In terms of objectives, hackers are not always out to steal data. Cyber espionage—hacking by nation states—for instance, is usually carried out to control the narrative, to cause damage, or to gather intelligence. Sometimes, hackers are just out to play pranks on random people. On other occasions, they've also been known to use their skills to make political statements.

Website defacement, a type of hacking that has been very prevalent during this pandemic, has been used a number of times to make political statements or to express popular public sentiment. It's been carried out by hacktivists railing against social and political injustices, like government incompetence and poor delivery of service. Others have sought to highlight the poor security of websites containing sensitive or critical data. In the case of the latter, even the National Privacy Commission's website was not spared.

Still, there has been no shortage in individuals that genuinely harbor bad intentions. Some of them have gone on to unlawfully access personal data that were then were sold to unknown third parties or used to access members-only sites. One example involved the exploitation of a misconfiguration of a particular government website, which then allowed the hacker to create a fake website. Nobody knows exactly how long the faux website was up before it was taken down.

An Enabling Environment

There are many reasons why phishing and hacking are such a regular occurrence these days. With phishing, it's usually because most people are incapable of distinguishing authentic communication from the fake ones. It certainly doesn't help that phishing attacks are increasingly becoming sophisticated, such that even those with some knowhow still end up victims sometimes. The Equifax case is a good example. Back in 2017, the company's official account actually tweeted multiple times the link to an identical yet fake Equifax website, even as it tried to warn clients about the very same fake website.

Policy-wise, the Philippines has several laws that protect critical infostructures, devices, individuals, and their personal data against all sorts of cyber attacks. They include the Data Privacy Act, Cybercrime Prevention Act, the Electronic Commerce Act, and the Access Devices Regulations Act. There is also a National Cybersecurity Plan (NCSP) which has for its objectives the raising of people's awareness about cybersecurity and ensuring the stability and resilience of government infostructure. Their effectiveness, though, is suspect, as may be gleaned from the uptick in internet crimes. Updates regarding the implementation of the NCSP are unavailable, preventing any measure of its positive impact. Even arrests of supposed hackers have offered little comfort, as many are later released due to lack of evidence.

Prioritization is also a big factor. Out of 76 countries, the Philippines ranked 29th in the least cyber-secure country in the world in 2020. Many establishments do not have the means to invest in the security of their IT resources or they simply don't want to. They find it too expensive, compared to the costs of a potential breach. Educational institutions are particularly notorious for scrimping when it comes to their cybersecurity measures. It's why few people were surprised when, last year, the scanning of school websites by a group of gray hat hackers revealed that around 20 schools were very vulnerable to online attacks. What made it worse was that even after school administrators were informed of the vulnerabilities, only some took the time to fix them.

As for government, the focus of the current administration, remains with infrastructure and defence programs. In a budget hearing, the PNP Anti-Cybercrime Group (ACG) highlighted the need for more funding in order to combat the influx of cybercrime cases during the pandemic. While the PNP's budget proposal of 2% increase was approved, it does not say how much is allocated to the ACG. If one were to scan the agency's strategic objectives for the current year, none of them is directly attributable to cybercrime prevention or resolution. Meanwhile, the Department of National Defense's cybersecurity fund was questioned by the Senate in a budget hearing for providing very little information about its operationalization. There are also no readily available reports that would allow one to gauge the effectiveness and progress of the ACG's and DND's cybersecurity operations over the years.

Finally, there is still the remarkable deficit in the number of cybersecurity professionals in the country today. Many attribute this to the lack of education opportunities on relevant fields like cybersecurity, information security, and data privacy. Those keen on immersing themselves in these subjects often have to go abroad, and tend to stay there—sometimes for good.

Playing catch-up

If the country wants to insulate itself effectively from hacking, phishing, and other cybercrimes, it will have to keep up with the rate of digitalization expected in a post COVID-19 environment.

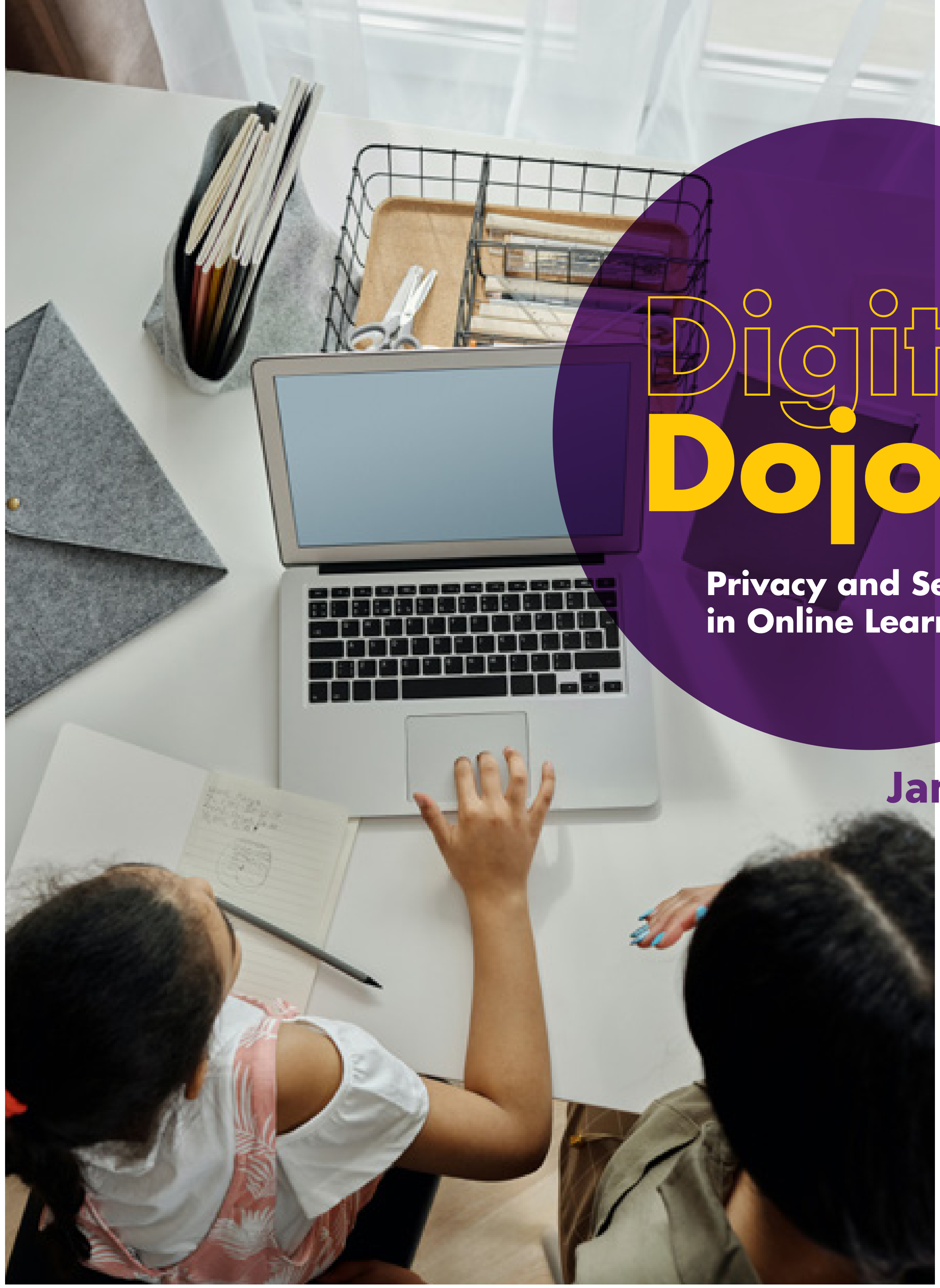
It can start by taking the regular cybersecurity reports issued by the government seriously and using these to craft appropriate responses. Relevant policies and standards have to be established by the concerned agencies, in consultation with other stakeholders in the private sector and civil society. Guidelines have to be both robust but malleable (i.e., capable of evolving along with the technologies they regulate). Of course, privacy should not be made a casualty of any effort to introduce improvements in cybersecurity.

In terms of focus, it's possible for one set of initiatives to zero in on the government and its peculiarities, and another to cater to critical industries in the private sector. Regulators need to be wary of emerging policy gaps, including the need for accreditation or registration mechanisms. The government accreditation of cloud service providers is a good example.

To complement state initiatives, the rest of government and organizations in the private sector will also have to make the necessary investments. They will have spend on security in order to attain security. That means establishing the necessary support infrastructure, procuring relevant security programs, and hiring or developing competent security professionals. After all, it's not only their institutions that are at risk, but also the lives and welfare of the people they serve or cater to.

Some emphasis should be given to the development of reliable training and certification programs in the country. At the moment, there are already efforts to address this concern, such as the recent introduction of a degree on Cybersecurity. There is also a plan to integrate the subject in the curriculum for senior high school. It bears stressing that the need to bridge the skills gap is of utmost concern and should be addressed the soonest.

For individual users and the public, in general, their share of the responsibility has been there right from the start. We, too, need to keep ourselves informed and updated of the latest security issues, including the proper way to deal with them. Malicious actors will always want to be a step ahead of everyone, and we really shouldn't make it easy for them to do that. If we do end up becoming victims, despite our precautions, we need to assert our rights fully and file cases, whenever appropriate. We need to stick with them, too, and not waver. A lot of cases are dismissed because the complainants themselves refuse to cooperate or lose interest rather quickly. If we do our part, we can be sure that we are already one step closer to managing this online outbreak.



Digital Dojos:

Privacy and Security in Online Learning

Jam Jacob

Amid the chaos wreaked by a raging global pandemic, documents featuring Social Security Numbers, student grades, and other personal data were stolen from a public school in Las Vegas, USA, by an unidentified hacker who later published them online. Apparently, the school was a ransomware victim and its officials had refused to pay the amount being demanded by the perpetrator.

That story is like countless others that have highlighted the woeful plight of educational institutions during this crisis as far as upholding the privacy and security of their constituents.

To be fair, most of their problems predate COVID-19. These things did not simply come out of thin air. It's the scale (i.e., in terms of speed, scope, and impact), though, that has caught many off guard. That and the rapid shift to online learning the pandemic has forced upon them.

A major concern is the way the transition has made school systems heavily dependent on technologies, especially the internet. The more central their role become, the more data they also crave for. Individuals and their personal data then become more exposed to the risks technologies have for baggage. It's the kind of scenario that led to today's data protection laws.

> ***A major concern is the way the transition has made school systems heavily dependent on technologies, especially the internet. Individuals and their personal data then become more exposed to the risks technologies have for baggage.***

Mapping the risk landscape

So far, the most prominent issue has been the increase in hacking incidents involving school websites and related information systems. In July 2020, the National Privacy Commission (NPC) noted a substantial uptick in the number of data breaches involving colleges and universities. Among the victims were the Polytechnic University of the Philippines (PUP), Far Eastern University (FEU), and the University of the Philippines Cebu. With PUP, the school said that no sensitive personal information were compromised. FEU was less fortunate, claiming that around 1,000 student accounts were made public, including details like names, student numbers, and passwords. For UP Cebu, administrators clarified that its student database was not connected to the compromised system. Still, though, information like the students' names and ID numbers were exposed.

Website defacements, in particular, have been rampant. Just these past couple of months, five schools had their websites defaced, including the Philippine National Policy Academy (PNPA). With PNPA, the hackers claimed that they accessed the personal data of more than 23,000 users.

Another phenomenon that gained notoriety was "Zoom bombing", or the practice by strangers of disrupting online gatherings or events, usually by performing offensive or lewd acts. In one incident, a grade 5 class was interrupted when an individual shared a malicious photo and exposed his private parts on screen. An online discussion hosted by a student organization was also trolled by a stranger who ended up flashing footages of Nazi propaganda.

Duplicate or fake Facebook accounts also became an issue when people began accusing them of sending threatening messages to the original accounts, many of which belonged to students opposing the country's controversial anti-terrorism law. While some suggested that a mere glitch could be behind the anomaly, they could not explain the harassment and other similar activities. Several government agencies committed to look into the matter, including the NPC, the Department of Justice (DOJ), the Philippine National Police (PNP), and the National Bureau of Investigation (NBI).

Further complicating things has been the inability of schools and students to adapt due to lack of resources. Most schools do not subscribe to learning management systems (LMS) and video-conferencing platforms. Not all teachers have computer units at home. Among those who do, some have devices that do not meet the minimum technical requirements. This is true for students, as well. Many are unable to afford a computer, or even a tablet or mobile phone, which they can use for schoolwork. Given the massive losses in livelihood the pandemic has caused, the situation has only gotten worse.

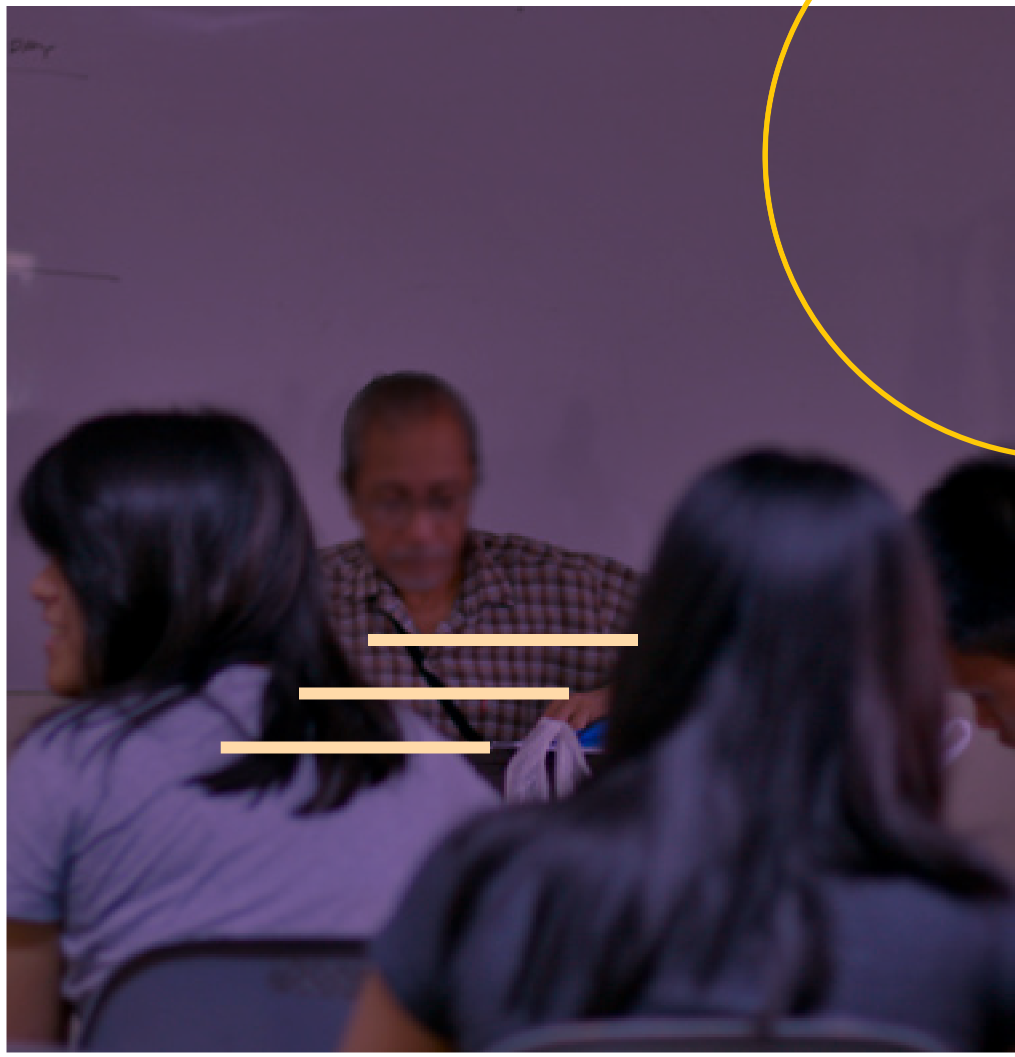
Topping things off is the country's poor internet infrastructure. Access to computer devices is one thing; making sure they are wired to the web is another. At present, access to technology is still a major concern for Filipinos many of whom still live in remote areas that do not even have electricity. It's a problem the Philippines shares with other countries. According to Save the Children International, at least 10 million students around the world were not expected to return to school in 2020 due to lack of access to technology.

Meeting the challenge (but coming up short)

Considering the surge in internet crimes, government response leaves a lot to be desired. Law enforcement authorities have reported very few apprehensions in the wake of the break-ins and other offenses. There was that time when the NBI supposedly arrested a 21-year old hacker for allegedly breaking into the accounts of at least 100,000 students, but apart from that, even updates on the reported incidents have been scarce.

Instead, it has been guidelines, advisories, and reminders–one right after the other–that has hogged the headlines.

Take the case of the NPC. After noticing the spike, the agency called on school officials to fortify their information



systems. Educational institutions, it added, should prioritize the security of their IT infrastructure, while making sure to adopt a "privacy by design" approach in the process. In October 2020, the agency came out with its Bulletin No. 16, which featured "Privacy Dos and Don'ts of Online Learning for K-12 and college students, parents, parents, guardians, teachers, and schools". Among those it recommended were oft-cited advice given by security professionals, like: (a) creating strong passwords; (b) using customized backgrounds during conference calls; and (c) turning off one's webcam and microphone during breaks. The NPC also cautioned against common risky practices like connecting to public WiFi networks and the unsanctioned taking of photos or videos during classes.

Just recently, the Commission updated its guidelines via a press statement. It emphasized the importance of having relevant policies (e.g., a social media policy) that always adhere to the principles of transparency, legitimate purpose, and proportionality, and which have the best interests of students as primary consideration. It suggested limits on the use of online messaging platforms and webcams for online learning. With webcams, there should be a policy in place to make sure their use is not abused. The agency also urged schools to explore alternative ways to monitor classes and exams and to observe other child protection policies.

The DOJ also went out of its way and came up with its own recommendations. In September 2020, the Department's Office of Cybercrime issued a public advisory regarding online classes that make use of video conferencing platforms. While the agency acknowledged video conferencing services "open doors to new opportunities that make access to education easy", it pointed out that such platforms also cause numerous security risks, including the "loss of confidentiality, availability, and integrity of computer data" and students' exposure to online criminals and harmful content.

Sitting on top of the pile has been the set of guidelines offered by the Data Protection Council (DPC) for the Education Sector. Sector-based DPCs were launched by the NPC in 2018 as a stakeholder approach to regulatory compliance and advocacy work. The said guidelines also feature a lot of common security measures, except that, compared to other issuances, their scope is far broader. They then manage to take up more specific concerns peculiar to the sector. It's worth noting that despite being an informal organization and having no real authority or power to impose rules, a DPC's inputs are relevant since it is composed of actual data protection officers representing the sector or industry. That said, their contribution is still just one more addition to an already substantial chorus of recommendations being offered by the government.

Meanwhile, to address the digital divide, state authorities have been promoting flexible learning programs that cater to both those who can afford to take online courses in full and those who need offline modes of learning delivery. Equipment-wise, an official of the Department of Education claimed in August 2020 that around 93% of all public schools in the country already had the devices needed for online learning. Teachers have also been given access to LMS so that they could create and schedule online classes, as well as other collaborative tasks. Other steps taken include the issuance of official email accounts for all elementary and high school students, and the training of teachers on ICT-based teaching. It is unclear, though, how much of these is reflected in the private sector. It is also painfully obvious that most of these actions—assuming they're all true and accurate—only address one aspect of the problem. They offer little to no help to students who cannot afford to purchase computer units for school use, or who live in regions that are without internet access.

A difficult path forward

When one takes stock of the situation, the considerable disconnect between the enormity of the problem and the available remedies currently being pursued is easy to appreciate. The transition to online learning has certainly caused privacy and security issues, while reinforcing and even expanding a lot of existing ones. A long-term viable solution should be based on a full appreciation of this fact.

The current one being implemented is not. So far, remedial measures have centered around persistent and often overlapping reminders from government agencies and sectoral representatives. There is little indication that more concrete steps are being taken, not just to prevent or avoid some of the problems, but also to bring to justice those responsible for online crimes and offenses.

Victims, too, need to change just as much. Their actions often betray their own claims of being responsible actors, wary of the dangers that surround them. Indeed, many educational institutions continue to show a preference for convenience or ease of use—over privacy and security—as the primary criteria for selecting products and systems that make their vision of an ideal online learning environment possible. This same approach explains why they have also been quick to rely on platforms that are not primarily designed for educational use (e.g., social media). Not only do these channels lack children's privacy standards, they may also be engaged in data processing that is either excessive or completely unwarranted (e.g., for commercial use).

What is needed is a balanced approach that solicits inputs and solutions from all stakeholders—legislators, regulators, schools, parents, service providers, and the students themselves. They all need to acknowledge that securing online learning environments is a complex project. It will take time before they can get everything moving towards the right direction. If they can agree to that, they will have already hurdled the first and biggest obstacle.

From there, they must scrutinize the current approach with an objective mindset and identify its deficiencies and their numerous failings. For this purpose, they can already adopt some of the observations presented here, like focusing too much on soft policies and reminders. There's already too much of that and too few consequences for those who refuse to heed recommendations. To be sure, policy gaps do still exist. But they need to be addressed by a comprehensive menu of solutions that assigns tasks to specific stakeholders. If additional manpower and resources are necessary (to increase the prosecution rate of malicious actors, for example), law enforcement authorities must work closely with policymakers to facilitate adequate funding. A clear menu or blueprint avoids confusion during implementation and also fosters transparency and accountability—both of which are also frequently absent in today's range of solutions. To achieve sustainability, there should also be a schedule for assessments that will allow for adjustments meant to address any setbacks encountered.

It seems like a lot, but it isn't really if seen from a proper perspective. Schools are indeed under a lot of pressure to get things right: provide quality education while upholding the privacy and security of their constituents. But as has been pointed out, that is a mission that will take some time, along with experience and hard work. There are no quick fixes. If everyone involved keeps that in mind, the task is manageable and a safe online learning environment is no longer just one person's pipe dream.

ID VS COVID

Locating the role of PhilSys within the COVID-19 pandemic

Jess Pacis

The COVID-19 pandemic has shifted everyone's priorities. As the world spins on and people learn, little by little, how to rebuild and rethink their lives around this so-called "new normal," the long wait for a cure for the novel coronavirus continues.

But while the possibility that a cure will be coming anytime soon is quite bleak, the Philippine government appears to be under the illusion that there is one magic pill for effective COVID-19 response: the Philippine Identification System (PhilSys).

The PhilSys was formally established with the passage of Republic Act No. 11055 in 2018. It is the product of a decades-long attempt to implement a mandatory and comprehensive identification system in the country. In 2020, long after the law and its implementing rules were signed, pilot registrations were conducted by the Philippine Statistics Authority (PSA) in preparation for a nationwide public rollout.

But then the pandemic happened. It significantly hampered the system's registration drive owing to the continuing state-imposed lockdown. Registration requires some degree of physical contact because of biometric data collection. Exactly the kind of thing people are being told to avoid to keep themselves safe from viral infection.

By late 2020, the PSA reported that only 10.5 million applicants had completed the first phase of registration it's a far cry from the target of having all citizens registered by the end of the Duterte presidency in 2022. On top of this, the PSA has also had to deal with a number of controversies, including one involving its procurement process for the ID system.

To date (April 2021), the registration process is supposed to be ongoing in varying stages in select regions of the country.

Surprisingly, despite all the setback, the PhilSys is mentioned regularly in the news as a major part of the country's solution to the global pandemic. Government agencies and officials have frequently cited the system when proposing or commenting on the administration's COVID-19 response initiatives.

Potential Uses

One of the first measures adopted by the government to contain the spread of the virus was a contact-tracing scheme. It was accompanied by suggestions from some parties regarding the linking of the PhilSys to the scheme. To them, it made perfect sense that PhilSys be brought up since contact-tracing relies on a system that allows the verification of people's identities, as well as the monitoring of their activities.

So far, though, it has been all talk. Nothing concrete has ever came out of the those remarks. The national government has never managed to develop a harmonized and comprehensive contact-tracing solution. Meanwhile, local government units (LGUs) have come up with their own contact-tracing systems, facilitated by their own data repositories.

Some LGUs have even set up their own ID systems. On January 2021, Quezon City launched its QCitizen, which is described as a "unified ID system" for city residents that allows for the availment of government services, including the future distribution of COVID-19 vaccines. Mayor Joy Belmonte describes the ID as "almost the same as the National ID that will be implemented by the national government".

Needless to say, initiatives like this, while addressing valid and pressing concerns at the local level, actually defeat the purpose of establishing a unified ID system that is supposed to eliminate the need for multiple means of identification.

There have also been talk of using PhilSys for aid distribution. The Department of Social Welfare and Development (DSWD) has claimed that the system could be a solution to the delays in the distribution of government assistance via initiatives like the Social Amelioration Program.

The National Economic Development Authority (NEDA) noted, though, that it will likely require the registration of families with PhilSys—instead of individuals. A prospect not aligned with the design of the ID system, as prescribed by law.

Supporters have not been limited to government agencies. Organizations like the World Bank also think it is a good idea. Across the globe, the institution has been dispensing massive funds to digital identification initiatives for COVID-19 response. In September 2020, the institution approved a US$600 million loan for the Philippines Beneficiary FIRST (Fast, Innovative, and Responsive Service Transformation) Social Protection Project. It involves helping the DSWD fast track PhilSys registration and promotes digital payment systems for government-to-persons transactions and the use of both the PhilSys and the National Household Targeting System database in building a unified beneficiary database. The Bank has also played a key role in the implementation of the Pantawid Pamilyang Pilipino Program (4Ps), which is also overseen by the DSWD.

At this point, it's worth noting that the banking and finance sector has always been a strong proponent of a unified ID system, arguing it would help facilitate financial inclusion. When the pandemic hit, it ramped up its call to have the PhilSys implementation expedited, as commercial transactions became increasingly reliant on digital platforms, while health and safety precautions led to a greater demand for contactless payments.

This remains true today, which could explain why PhilSys has included in the E-commerce Philippine 2022 Roadmap that was launched early this year. One of the core strategies identified in the document is the speeding up of eGovernment initiatives across the e-commerce ecosystem, including PhilSys implementation.

More recently, the PhilSys is also being floated as a possible tool for vaccine distribution. The NEDA appears to be the primary proponent, with some lawmakers also throwing in their support. NEDA's involvement is critical since its head sits as Chairperson of the PhilSys Policy and Coordination Council (PSPCC), while the agency itself is a member of the National Task Force against COVID-19.

Meanwhile, local digital ID systems like the QCitizen are also being marketed as potential vaccine distribution tools. The only thing that has kept matters from going further is the delay in the actual arrival of vaccines, and public distrust in vaccines themselves.

> ***"...the banking and finance sector has always been a strong proponent of a unified ID system, arguing it would help facilitate financial inclusion."***

ID Systems in COVID-19 response abroad

Of course, using identification systems in support of state-initiated pandemic response projects is not a novel idea, and is certainly not unique to the Philippines. That said, the experience of other countries appear to confirm that the proposal is saddled with issues and a lot of possible complications.

In India, citizens are required to link their mobile number to their Aadhaar card in order for them to avail of COVID-19 vaccinations. This move continues to face overwhelming backlash from stakeholder groups. Rethink Aadhaar, a campaign that challenges the ID system, has highlighted several privacy concerns regarding the linkup. Among them is the lack of privacy safeguards in both the mobile application to be used and the vaccine delivery system as a whole. They also cite a violation of the purpose limitation principle in data protection, particularly the use by the government of the vaccine delivery system to populate the Digital Health ID database without the consent of the data subjects. There is also the possibility that the plan would disenfranchise unregistered citizens and those who do not have their mobile number linked to their ID—a clear violation of the universal right to health.

Meanwhile, for Venezuelans, the threat of an ID system leading to social exclusion is all too real. In their country, they are required to possess a Patria or "fatherland card" to be able to receive social benefits. Even before the pandemic, the Maduro regime was already exploiting the Patria system to exercise social, economic, and political control over the population. Things got worse during the pandemic, as evidenced by the spike in cases involving government harassment committed against health care workers, human rights defenders, journalists, and migrants.

Ireland's Public Services Card (PSC) is another example. In the early months of the pandemic, United Nations Special Rapporteur on extreme poverty and human rights, Philip Alston, criticized the PSC for making public services and benefits less accessible to marginalized populations because of its strict documentary requirements. He noted that, although the government eventually waived the PSC requirement for some COVID-related benefits, it cannot be denied that the system does tend to discriminate against the poor and the disadvantaged.

A Way Forward

The nationwide implementation of a national ID system during a pandemic is no small challenge, and all the more so if it is to be done in a way that is inclusive and respects fundamental rights. Still, several other countries are taking on the task now. From them, Philippine authorities have an abundance of global experience and lessons to draw from when implementing the PhilSys.

With the World Bank taking the lead, a group of organizations came together in 2017 to craft a set of principles (ID4D Principles) to guide the development of identification systems that are inclusive, trusted, accountable, and aligned with the Sustainable Development Goals. Drawing from actual experiences and lessons in the implementation of ID systems around the world, an updated version of the Principles were released in 2021, divided into three major pillars: Inclusion, Design, and Governance. Since the PhilSys project framework was supposedly anchored on the Principles, the updated version is a good starting point when thinking about ways to ensure the smooth and responsible implementation of the PhilSys.

- **Inclusion.** An inclusive ID system ensures universal access for individuals and removes all potential barriers to its use, including financial costs and technology gaps. The very essence of a foundational ID relies on the scope of its use cases and the number of users in a given population. PhilSys was designed as a way to improve access to government services. To fully serve its purpose, the system should be within reach of as many citizens as possible. This becomes more important now, given the suggestions that it be used as a tool to facilitate vaccine distribution. So far, there are still implementation issues that have yet to be addressed properly, like the significant chunk of the population that don't have the basic requirement: a birth certificate. The system's implementing rules attempted to address this through an "introducer" mechanism, which allows a registered individual to vouch for the identity of a PhilSys applicant that does not have a birth certificate. However, now that registration is already in motion, there have been no further information regarding the use of this mechanism.
- **Design.** The ID4D Principles, as well as RA 11055, mandate that PhilSys should be designed in such a way that would ensure the people's right to privacy and confidentiality. Apart from the security measures provided by the PhilSys law, it must also abide by the fundamental principles of data protection under the Data Privacy Act. To minimize confusion and the possibility of function creep, the PSA must establish clear terms that would govern the proper use of the PhilSys. The ID4D Principles also endorse the creation and use of a responsive and interoperable platform, as well as the use of open standards. These standards must be followed not just in the creation of the main PhilSys database itself, but for any other platform that will be developed and integrated with it. For example, there have been reports that the PSA intends to open an online registration portal by April 2021 to ramp up the process despite COVID-related restrictions. Such a platform adds to the overall PhilSys framework and must be designed with the same standards as the main one.
- **Governance.** As per the principle of governance, there must always be clear institutional mandates and accountability. Independent oversight and the adjudication of grievances must also be enforced. In the case of PhilSys, there is an urgent need to identify the limits of data-sharing between agencies and to ensure that every entity—including private contractors—that will be given access to the system is equipped with the necessary privacy and security measures. As with any other government response to the pandemic, the success of the PhilSys also relies on the cooperation of all stakeholders. Such harmony is especially crucial in ensuring synergy between their respective security measures. Finally, transparency should be practiced not just in the documentation of data-sharing arrangements, but with every other aspect of the system's implementation. For now, apart from the frequent press releases about the number of registrants, very little information is being disclosed to the public insofar as what goes on behind the curtains of the PhilSys rollout. One can only hope that by the time registration is completed, all registered individuals are treated not just as providers of information, but as empowered participants and collaborators in the nation's identity-building process.

Policing Online Spaces

Jam Jacob

> *"Indeed, the prospect of having social media governed and monitored by the state's armed personnel is something any reasonable person would treat with great trepidation."*

In September 2020, the Joint Task Force (JTF) COVID Shield, in coordination with the Philippine National Police, ordered all police commanders to monitor Facebook and other social media platforms for possible violations of prescribed health protocols, such as motorcycle "back-riding", drinking sessions, parties and other forms of celebrations, and other mass gatherings. The call was supposed to complement similar efforts on the ground that form part of the government's overall response strategy relative to the COVID-19 pandemic.

The announcement elicited sweeping public condemnation. Law enforcement authorities were already grappling with a deplorable public image, courtesy of their members who were constantly embroiled in all sorts of crimes, scandals, and controversies. News of them about to proactively keep track of the population's social media activities was widely regarded as yet another example of their propensity to abuse their powers.

Still and all, it's worth noting that social media surveillance is not a new phenomenon. It has been around for quite some time—perhaps even dating back to the moment social media itself was born. And it is undertaken by different parties that hail from a wide variety of sectors, representing all sorts of interests.

Schools, for instance, employ social media software to look for possible threats like students' posts that indicate suicidal tendencies or threats of gun violence. Employers are naturally interested in public posts of disgruntled employees that may cause reputational damage or disclose confidential and proprietary information. And then, of course, there's government which uses the data it scoops up for various purposes ranging from denial of immigration or naturalization applications, to arrests relating to crimes committed by people while on their social media accounts.

Nevertheless, this doesn't mean the practice has already risen to the level of a norm, one that has garnered near-universal acceptance from society. This is particularly true in the Philippine context where the Task Force announcement and the raging pandemic are just two more fuses added to the existing powder keg of issues confronting the administration of current President, Rodrigo Duterte. If not handled well, the outrage caused by the proposal could set off a series of irreversible consequences too great for the government to contain.

A chorus of criticisms

According to Cristina Palabay, Secretary General of human rights group, Karapatan, the proposed move by the police had no legal basis and was "nothing more than an insidious cover for online policing and mass surveillance".

That sentiment was echoed by the National Union of People's Lawyers (NUPL) who pointed out that the PNP cannot just start stalking people without being properly authorized by the courts. It is, after all, evidence-gathering carried out via surveillance tactics. There are prescribed legal procedures to be followed for that. The plan would also violate other laws, including the country's Data Privacy Act. Even if the statute grants exemptions in favor of public authorities, abuse by the latter of their mandate effectively revokes those exemptions as a necessary safeguard for the affected individuals and their personal data. The group also described the proposal as particularly worrying when put together with an equally recent proposal by the military to regulate social media. Indeed, the prospect of having social media governed and monitored by the state's armed personnel is something any reasonable person would treat with great trepidation.

The National Privacy Commission also weighed in and said that while the police may use social media to look for possible violations, evidence must still be obtained lawfully and people's data privacy rights must still be recognized. It recommended that the PNP utilize "non-invasive" techniques in conducting their monitoring work to make sure their actions remain consistent with data privacy regulations. The police, it added, should also explain how they intend to carry out their work to allay people's fears of mass and indiscriminate surveillance.

Another rights-oriented state agency, the Commission on Human Rights, reiterated the NPC's call for a more measured approach to surveillance. It advocated for techniques that are guided by the standards of necessity, legitimacy, and proportionality. Even in the midst of a national health emergency like the current pandemic, respect for and the protection of human rights are still paramount and cannot be simply set aside.

Among civil society groups, the Ateneo Human Rights Center was quick to assert that the controversy is also a due process issue. It noted that while social media monitoring may be argued as part of the PNP's mandate, people cannot simply be penalized or charged with health protocol violations based solely on online content. Those data can of course be used as evidence, but they still need to be validated or verified. Here, the prickly issue of credibility on the part of the PNP comes into focus. The institution should be able to convince people it is fair and objective when it enforces the law. Since many of its top officials have also been accused of violating health protocols—and managed to get away with it—questions regarding the moral authority of the PNP to enforce those same rules continue to linger.

It should be recalled that in May 2020, current PNP Chief, Debold Sinas, and dozens of other officers were caught on camera celebrating his birthday sans masks and openly disregarding physical distancing requirements. The PNP itself posted the photos online. Sinas and his colleagues briefly faced criminal charges before the Taguig Prosecutor's Office, but those cases were later dropped. Sinas even get promoted to his current post.

Clarifications and justifications

Needless to say, not everyone was convinced that the PNP would be acting beyond its mandate if it pushed through with its plan. As far as Executive Department was concerned, there was nothing wrong with the directive given. According to Presidential spokesperson, Harry Roque—who is a lawyer—a person's right to privacy in relation to any content he or she posts on the internet is essentially waived. He basically posited that once something is posted online, the world acquires the right to see it. A person won't be able to do anything about it, except not to put that material out there in the first place. He also pointed to the country's anti-cybercrime law, the Cybercrime Prevention Act of 2012, and noted that social media monitoring is not among the online activities prohibited by the law. In fact, as similarly noted by the Integrated Bar of the Philippines, the police actually has the power to check viral posts when looking for possible quarantine violations.

Before more people could offer their thoughts on the subject, the PNP leadership made a timely decision to step in and provide additional details about its earlier proclamation—presumably before things got really out of hand.

According to Police Lt. General Guillermo Eleazar, commander of JTF COVID Shield, the monitoring will actually be limited only to public posts, viral photos or videos, and complaints received by the police. The PNP will not engage in the monitoring of private social media accounts

precisely because it is illegal, as per the country's data protection law. Besides, he said, they currently have no capability to carry it out. The agency doesn't have the technology or the manpower needed to scour millions of social media accounts in search of potential violators of pandemic-related regulations. Eleazar also emphasized that social media posts won't immediately lead to arrests, since the ordinances of local government units favor community service and fines as penalties, instead of prison time.

The clarifications made regarding the scope of the surveillance appear to have appeased many critics. Most remain wary, however, given the police's history of deviating from its declared policies.

As far as Eleazar's statement regarding the PNP's current surveillance capabilities (or lack thereof), it is practically impossible to verify that at the moment. It would be best not to put too much faith in it, however, since very few governments would volunteer to disclose the full extent of their powers, if at all. That said, there is proof of sale of various surveillance equipment to the Philippine government during these past half decade. Previous leaks have also disclosed other possible transactions that may have occurred, like an attempt to obtain spying software from Italy's The Hacking Team and an offer by the New Zealand government regarding its Signal social media monitoring solution. One will simply have to take these into account when assessing the PNP's assertions.

In response to allegations that PNP personnel might circumvent or undermine laws in carrying out their orders, assurances were also made regarding the agency's compliance with the Data Privacy Act and its commitment to due process. The police will supposedly see to it that they look for other supporting evidence and witnesses to properly investigate violations. Fears of abuse were swept aside via a promise to make anyone caught abusing the system answer for their crimes.

Finally, there was a low-key attempt to shift the narrative by describing the measure as a way to actually empower the people. According to Eleazar, because citizens would be given the opportunity to report violations, they will not only help the government enforce quarantine rules, but also protect themselves and their community from "hardheaded" violators.

Asserting the line

Notwithstanding the PNP's remedial efforts, the organization still ended up being forced to take back its directive under the guise of clarifications that virtually gave hollow meaning to its original proclamation. The pushback from critics and the public at large became too intense that it had very little appetite left to insist on staying with its agenda moving forward.

That was something worth celebrating. The victory, however, would be for naught if people are unable to appreciate the value of the extensive public debate that hounded the controversy. Creating sufficient backlash was critical. The points raised are worth remembering, too, as they will surely be needed anew when this same subject is brought up again by the police based on what is certainly going to be a different pretext.

Moreover, it should also be clear by now that surveillance per se has a critical role in any government initiative designed to address public health crises like this global pandemic. Disease surveillance is a thing, and a necessary one, at that.

The worry for many is how authorities around the world have used the COVID-19 crisis to justify the expanded surveillance powers they have always craved for and the deployment of new technologies ordinarily regarded as too intrusive under normal circumstances.

In other words, the pandemic has created an opening for the introduction of large-scale data collection activities, with little to no pushback from civil society or the general public. After all, who would argue against a measure if it is being billed as a necessary step to arrest the spread of a deadly disease—one that still has no cure.

From there, the bigger danger lies in the possibility that all these new measures will become a permanent fixture in people's lives. History has shown that such moves, once in place, are extremely hard to scale back after the crisis they were meant to address is finally over.

For now, Filipinos are able to take comfort in the thought that they averted one attempt by the state to normalize social media surveillance. They should be prepared to do so again in the next round. Because there will definitely be another one.

Apps Rising

Maris Miranda

Did you know that the first mobile gaming app was the "Snake"? During its heyday, it seemed like everyone was into that game. And why not? You had a simple objective (i.e., to grow the snake without bumping into a wall or the snake's own body). There were no ads to distract you. Internet access wasn't even necessary.

That was decades ago. All apps had to be built into the phones and the App Store, as we know it now, was still just a concept.

Mobile apps have come a long way since then. No longer limited to gaming and simple productivity tools, they have become a huge part of our lives. They make many of our tasks so much easier to do, with just a few clicks, swipes, and taps on our devices.

At no point has this been more apparent than during this COVID-19 pandemic. Due to limited mobility, people have been forced to shift to digital platforms in order to meet most—if not all—of their daily needs. Naturally, companies have taken this opportunity to ramp up their app development to keep up with the surge in demand.

Rising apps

For the Philippines, a quick look at the top app downloads for both Android and Apple devices readily explains the impact of the health crisis on local app use.

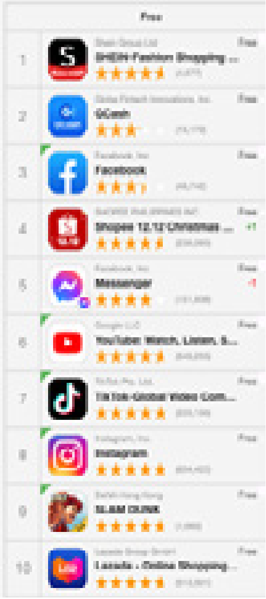
Among the most affected has been the population's shopping behavior. Use of shopping apps was highest in the ASEAN region during the second quarter of 2020. In the Philippines, Lazada, Zalora, and Shopee became the most visited online stores once the nationwide lockdown began.

Other fintech apps have benefitted, as well. Mobile wallets have become a necessity for many as more businesses direct them to online payments. GCash saw a 1000% increase in online money transfers, making it the top finance app in the country. Not one to get left behind, Grab and other companies have also expanded the use of their own mobile wallets.

Videoconferencing apps like Zoom and Microsoft Teams also saw their popularity soar, especially among schools and businesses, owing to their for regular interactions like classes and meetings.

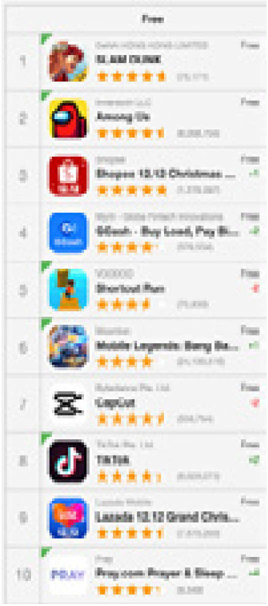
Of course, those apps designed to entertain remained in demand. Surrounded by sickness and financial troubles, people regularly turned to games, streaming services, and social media platforms for comic relief. TikTok, in particular, has been a big hit among the so-called Gen Z.

Figure 1. Top free apps downloaded on iPhones in the Philippines (1 Dec 2020)



Free		
1	SHEIN-Fashion Shopping ...	Free
2	GCash	Free
3	Facebook	Free
4	Shopee 12.12 Christmas ...	Free
5	Messenger	Free
6	YouTube: Watch, Listen, S...	Free
7	TikTok-Global Video Com...	Free
8	Instagram	Free
9	SLAM DUNK	Free
10	Lazada - Online Shopping...	Free

Figure 2. Top free apps downloaded on Android devices in the Philippines (1 Dec 2020)



Free		
1	SLAM DUNK	Free
2	Among Us	Free
3	Shopee 12.12 Christmas ...	Free
4	GCash - Buy Load, Pay Bi...	Free
5	Shortcut Run	Free
6	Mobile Legends: Bang Ba...	Free
7	CapCut	Free
8	TikTok	Free
9	Lazada 12.12 Grand Chris...	Free
10	Pray.com Prayer & Sleep ...	Free

Source: Sensor Tower

A shift and a virtual minefield

Observers agree that the pandemic has significantly sped up the world's transition to e-commerce and e-services. It managed to do within months what would have otherwise taken years to accomplish.

It certainly helped that very little was needed to make converts out of people. The apps themselves did most of the convincing. Their selling point? Use of mobile apps is not only convenient but also safer—at least in the sense that you have a lesser chance of contracting the deadly virus.

Still, one would be remiss if one fails to acknowledge that the shift has many issues too. It shouldn't be a surprise. To make the expedited rollout possible, some companies must have cut corners and fast-tracked certain processes. Any time that happens, bugs and other flaws are a normal occurrence. There is also much to be said about the readiness of the Philippines' existing digital infrastructure. Simply put, it remains dismal compared to those of other countries.

Here's a peak at some of the hiccups encountered so far:

- **Data breaches.** A large number of apps have experienced data breaches that exposed their users and their users' personal data to a number of risks. SHEIN, Globe, Facebook, Instagram, TikTok and YouTube have all gone through a data breach. Messenger and Shopee both had bugs that could've also exposed their customers' data.
- **State surveillance.** Some apps have been accused of illicit surveillance activities done on behalf of state authorities. For instance, mobile apps owned by Chinese companies are often chastised because of China's reputation as a surveillance state. Many have been banned in India, including TikTok and SHEIN, for supposedly posing a threat to national security. The US attempted a similar ban but was blocked by its courts.
- **Unauthorized processing.** Apps, including major ones, have also been caught engaging in illegal data processing. Google was sued in the United Kingdom for tracking children online. Zoom was said to have unlawfully shared its users' data with Facebook. Grab, on the other hand, unlawfully collected user data via its pilot system.
- **Excessive permissions.** Few users are aware that their apps ask for a disproportionate amount of information in exchange for the services or features they provide. The apps manage to do this via permissions they request for prior to or during installation. Most developers adopt a take-it-or-leave-it approach, leaving people with no choice except to agree. Unfortunately, some permissions, if granted, are really quite dangerous. For instance, the "draw over other apps" permission may allow a hacker to disguise a malware as a fake ad.

- **Excessive data sharing.** Many apps give new users the option of signing up using an existing social media account. This often entails the sharing of their personal data between the companies involved, including the latter's affiliates and other third parties. Through the shared information, businesses are able to create more accurate user profiles, which can be transferred or even sold to other entities. Worse, this also means the impact of any data breach affecting said profiles will be that much greater.
- **Poor transparency initiatives.** Even attempts by apps to comply with regulations often come up short. Take the case of privacy notices that are often too long and riddled with technical, legal jargon. People don't even bother to read them, anymore. According to one study, many of these documents exceed the college

reading level. Whether or not this is intentional on the part of the companies that prepared them, the purpose behind these documents is unavoidably undermined, if not outright defeated.

Compounding matters are issues that affect the way these apps operate. Foremost among them are the varying regulatory regimes in place and the existence of weak ones. Because of the former, companies end up treating their users differently, as determined by their location or nationality. Facebook, for instance, only expressly allows those covered by the EU-US and Swiss-US Privacy Shield Framework to opt-out of third-party data sharing and processing activities not related to the declared original purpose. Tiktok also has location-specific provisions, most of which favor those residing in jurisdictions like the United States, Switzerland, and the European Economic Area.

As regards weak regulatory environments, it's worth noting that while some view regulations as unfairly restraining innovation, they are very much necessary if organizations are to be kept honest, and the technologies they produce, safe and secure. It all starts with a sound regulatory environment. In the Philippines, it's difficult to say which agencies are supposed to keep apps in check. Is it the Department of Information and Communications Technology (DICT)? Maybe the different Departments are responsible for their respective sectors or fields? Does the National Privacy Commission (NPC) have a say in it, too? How about local government units? With no clear framework, app developers have had to deal with multiple regulations and requirements. Sometimes, they overlap. Sometimes, they contradict each other. The problem goes all the way up to enforcement. Some regulators are inexperienced, while others are ill-equipped. In the case of the NPC, there are those who wish the agency is more proactive in its compliance work. This includes having a proper Schedule of Fines so that violators get more than just a slap on the wrist when they are caught breaking the rules.

Forging ahead

All these problems (and more) notwithstanding, mobile apps will remain a fixture of modern life. At this point, it's already impossible to decline the opportunities, convenience, and safety they provide. What we have seen, though, is that all of its benefits come with a price. If not handled properly, that price may prove more costly than the alternatives we have traded away in exchange for these apps.

To keep that from happening, the government has to step up and establish a more reliable regulatory regime; one that does not impede innovation and new technologies. It cannot allow the private sector, especially the so-called big tech companies, to set the rules. It can lay down the groundwork by setting the minimum security standards and data protection measures that apply specifically to mobile applications. Regulators should work with other stakeholders for a more inclusive and more effective policy-making process.

Policies won't be enough, though. They can be useless if authorities do not have the resolve to implement them. In the case of regulators like the NPC, it's hard to put a premium on their resolve without them having any record of actually penalizing anyone for violating regulations. If the NPC needs a Schedule of Fines for that, it should work double-time to issue one as soon as possible. Other agencies like the DICT should follow suit and also build up their capacity, in terms of skills, manpower and facilities. They need to work closely with their foreign counterparts since many apps belong to companies located outside the country. Cross-border cooperation will be crucial.

App developers also need to carry their own weight. These are their products, after all. Accountability demands that they make sure these things do not cause harm or put people at risk. To their credit, some are doing a few things now. Google and Apple, for example, have set limitations to the permissions they allow. To assist users further, Apple is also now requiring developers to upload a Privacy Nutrition Label that summarizes the data they collect and how they use it. Some have welcomed this development, while others criticize it for stifling competition. These things represent a good start; but are nowhere near the effort we must expect from these organizations.

Civil society organizations will always have a role to play, too. At the moment, one great initiative worth continuing (and expanding) is the ToS;DR project, which aims to raise public awareness regarding data privacy, while calling out companies and government authorities that fail to uphold people's rights.

As app users, we ought to be more responsible as well, even as we continue to avail of the benefits these programs provide. At the very least, we should inform ourselves of what we are getting ourselves into by actually reading privacy notices and the terms and conditions governing their use. Let's also be more mindful of the permissions we agree to.

In the end, it's best to keep in mind that while mobile apps have proven themselves useful, fun, and often easy to use, they remain tools made by third parties that we have allowed into our lives through devices we carry around practically everywhere. Just like any stranger we meet, they will have to gradually earn our trust, by handling our data responsibly and by keeping us from unnecessary risks.

Securitization as COVID-19 Response

Jess Pacis

It's 2021 and we all know the COVID-19 pandemic still looms heavily over our lives. Despite this, we have to be wary of another lurking threat that hopes to remain unnoticed even as it stifles our most basic freedoms at a time when we need them the most. They are the laws that restrict the exercise of our human rights.

Just when the free flow of information and public discourse are most crucial, the Philippine government has put a premium on silencing and harassing the population, especially its critics and the press.

In 2020, the country ranked 136th out of 180 countries in the World Press Freedom Index, dropping two places from 2019. Its score in the Freedom on the Net rankings also dropped from 66/100 in 2019 to 64/100 in 2020. The scores there are based on a scale of 0 (least free) to 100 (most free). This means internet freedom in the Philippines is partly free, attributable to factors such as the shrinking space for critical speech online, ramped up arrests of online users amid the pandemic, online harassment of government critics, and technical attacks against media and civil society.

To be sure, the Duterte administration has always been antagonistic towards free speech and a free press. However, things took a turn for worse during the COVID-19 pandemic, after the government transformed the public health crisis into a large-scale narrative of terror. It began by adopting a highly militarized strategy for its pandemic response, appointing former generals to head the National Task Force charged with implementing the National Action Plan against COVID-19. The move was consistent with Duterte's penchant for hiring retired military men to key leadership positions in his cabinet.

This approach was bolstered by the use of laws—both old and new—that expand the powers of law enforcement and the military when it comes to controlling public discourse and suppressing government criticism.

Bayanihan Act

On 24 March 2020, President Rodrigo Duterte signed Republic Act No. 11469 into law. It has for its full title, "An Act declaring the existence of a national emergency arising from the Coronavirus disease 2019 (COVID-19) situation and a national policy in connection therewith, and authorizing the President of the Republic of the Philippines for a limited period and subject to restrictions, to exercise powers necessary and proper to carry out the declared national policy and for other purposes". Today, it is often referred to as the "Bayanihan 1".

One controversial provision of the law penalized "individuals or groups creating, perpetrating, or spreading false information regarding the COVID-19 crisis on social media and other platforms, such information having no valid or beneficial effect on the population, and are clearly geared to promote chaos, panic, anarchy, fear, or confusion; and those participating in cyber incidents that make use or take advantage of the current crisis situation to prey on the public through scams, phishing, fraudulent emails, or other similar acts." Civil society groups and lawmakers wasted no time in pointing out the dangers of this particular provision—particularly, that it suppresses freedom of speech and that its vague language allows possible misuse and abuse by State actors.

The impact of the law seemed immediate. Mere days after it was signed, 32 arrests had already been made in connection with the supposed spreading of disinformation online regarding COVID-19.

Curiously, the first of those arrests involved supposed violations of the country's Revised Penal Code (i.e., "Unlawful Use of Means of Publication and Unlawful Utterances"). This, despite Bayanihan 1 being in effect already at that time. Equally surprising was the fact that the controversial provision would be noticeably absent in the replacement law ("Bayanihan to Recover as One Act" or "Bayanihan 2") that took effect in September 2020, and in the third version (i.e., "Bayanihan to Arise As One Act"), which is currently pending in Congress.

Anti-Terrorism Law

This link between free speech and privacy, as well as the escalating abuse of State power in the name of public security, peaked with the enactment of Republic Act No. 11479 or the controversial Anti-Terrorism Law (ATL). It expands the definition of terrorism, while increasing the counter-terrorism powers of uniformed personnel. After the law was signed, petitions piled up before the Supreme Court as they sought to challenge the law's constitutionality. Another contested feature of the law is how it makes it easy for security forces to conduct lawful communication surveillance and how it eliminates the safeguards previously contained in the now-defunct Human Security Act. The state's reinforced surveillance powers violate the constitutional rights to privacy of communications and against unreasonable searches and seizures.

As was the case in the first Bayanihan law, the ATL's negative impact on human rights, especially those of the marginalized sectors, was immediately palpable. The first publicly known case under the law involved two Aetas (i.e., members of an indigenous group) who were charged with terrorism for allegedly shooting at soldiers. One of the petitioners against the law was also arrested at a school for lumads (i.e., another indigenous group) for allegedly recruiting children into a communist group. Meanwhile, other petitioners called the attention of the Supreme Court to the alleged profiling and intelligence-gathering activities being carried out against them by the government.

As of this writing, the oral arguments on the law being heard by the Supreme Court have not yet concluded. The Office of the Solicitor General, on the other hand, continue to defer action on the motions filed by some petitioners seeking a Temporary Restraining Order against the ATL's implementation.

Cyber Libel

It's important to note, however, that prior to the passage of these recent laws, the Philippine government already had a powerful tool that allows it to crack down on speech that may be considered disinformation or defamation. The country's Cybercrime Prevention Act, which was passed way back in 2012, already penalizes online libel, as well as all other crimes committed with the use of ICTs. The crime of "Unlawful Use of Means of Publication and Unlawful Utterances" mentioned earlier would be one.

Perhaps the most famous local cybercrime case to date is that of Maria Ressa, a veteran journalist and founder of online news outlet, "Rappler.com".

During this pandemic, cyber libel has also been used against other journalists, cultural workers, and even ordinary citizens. Most of the cases supposedly involve some form of disinformation. They have led to an increase in related arrests, especially in the wake of Ressa's.

On April 19, Cebu-based film writer and artist, Maria Victoria "Bambi" Beltran, was taken into custody and charged for violating the

cybercrime law, the Bayanihan law, and the law on the mandatory reporting of communicable diseases. Her case stemmed from a Facebook post wherein she said that the 9,000 new Covid-19 cases in her city during one particular day all came from one area: Sitio Zapatera. She then referred to that locality as "the epicenter in the whole Solar System." While Beltran described her post as being satirical, the Mayor thought otherwise.

Also arrested were a public school teacher in Zambales and another teacher in General Santos City. Although eventually dismissed due to an invalid warrantless arrest, the inciting to sedition case against the Zambales educator originally stemmed from a tweet that offered a P50-million bounty to anyone who could kill President Duterte. Meanwhile, the teacher from General Santos City was accosted after she published on Facebook a post criticizing the local government for its lackluster response to the health crisis.

The phenomenon that is securitization

This inclination of the Philippine government towards draconian responses to the COVID-19 pandemic can best be described as a case of securitization, which occurs when a "soft" security issue (in this case, a health crisis) is declared by political actors as an existential threat and then used as justification to implement extraordinary and sometimes illegitimate issues.

This strategy isn't unique to the country. It enjoys widespread use all over the world, especially in states with authoritarian (or quasi-authoritarian) regimes. In Israel, for example, the government approved as an emergency measure the tapping into a trove of cellphone data to trace the movement of people who tested positive with the coronavirus. In Venezuela, the Maduro regime has used the health crisis as an opportunity to scale up government repression, with the cases of killings and violence against government dissenters having increased during the pandemic. The attacks were done after a state of emergency was declared by the Venezuelan government, as most governments did at the beginning to impose lockdowns.

"By now, most people have noticed that many physical attacks and acts of violence are preceded by privacy violations."

The same pattern is seen in other Asian countries. Some of them have also come up with emergency legislation similar to the Bayanihan law. Take the case of Thailand where the state of emergency provided the government with power to suspend or order the "correction" of any news that they deem untrue or problematic.

Wherever they are found, the danger they pose is real. Beyond the threat of arrests or harassment they give rise to, one also has to appreciate the chilling effect that they have on free speech. Here in the Philippines, a nationwide survey conducted in November 2020 revealed that 65% of adult Filipinos agree that "it is dangerous to print or broadcast anything critical of the administration, even if it is the truth."

Even the right to privacy is not spared. By now, most people have noticed that many physical attacks and acts of violence are preceded by privacy violations. Since the laws mentioned above also manage to legitimize a lot of State surveillance practices, many believe they share part of the blame for the deaths that have occurred this past year. If one looks at the local activists who have been killed during this pandemic—Zara Alvarez and Dr. Mary Rose Sancelan, for instance—most had previously complained of being victims of various types of privacy violations.

For Filipinos, this has become the grim reality. According to a report from Human Rights Watch, casualties of Duterte' war against drugs increased by more than 50% during the early months of the pandemic. The report also cites that "threats and attacks, including killings, against left-wing political activists, environmental activists, community leaders, Indigenous peoples' leaders, journalists, lawyers, and others" spiked in 2020.

Finding solutions

Violations of human rights disguised as valid COVID-19 response appear to be a conflation of a number of issues, ranging from press freedom, to state surveillance, all the way up to propaganda in preparation for the 2022 national elections. Accordingly, any type of response that hopes to achieve a considerable degree of success in addressing them must have a full grasp of the situation and look carefully into all those different issues.

Government watchdogs like the National Privacy Commission, which is the implementing agency for the country's Data Privacy Act, and the Commission on Human Rights should assume a central role in all ensuing discussions. They need to lead and pave a path that other government agencies and private actors alike can

trace and follow so that they, too, may implement the necessary measures in their respective domains.

Naturally, policymakers will have their work cut out for them. They need to get better at crafting laws. Policies should not have to sacrifice human rights in their pursuit of some other legitimate objective. Even in cases where this is unavoidable, the version that demands the least sacrifice should be preferred. One item that needs be revisited soon is the decriminalization of libel. While the crime exists, it will remain a significant concern for civil society, and especially for journalists, because it allows those in power to abuse the justice system for political and personal gain.

It's a lot a work, no doubt. This is why other stakeholders—from civil society, the academe, and the private sector—need to come together and support a genuine agenda for change. They cannot allow this matter to stagnate and turn into a mere afterthought. If they do, the next major crisis will just be another opportunity for even more draconian measures to be added in an already stacked government toolbox.

We, Filipinos, just like our peers in the other corners of the globe, deserve a legal framework and a government that both uphold our fundamental freedoms and protect us from other dangers like the current global public health crisis. We definitely need it now; but unlike the current pandemic, this need will subsist, tomorrow and beyond.

Trace to the Bottom:

Digital Contact Tracing in the Philippines

Jess Pacis

April 2020. A month after COVID-19 was officially declared as a pandemic. Governments all over the world were scrambling to come up with their own ways to monitor and contain the spread of the virus.

April 2021. Over a year since then. Countries are slowly recovering, economies are reopening, vaccines are being distributed, and the number of infections is being contained—except in countries like the Philippines, where new cases are at an all-time high. On April 2, the country set a record with 15,310 new cases logged in a single day.

What went wrong?

If you ask the experts, they could point to a myriad of things, but a large chunk of the problem dates all the way back to April 2020, when the Philippine government started developing its contact tracing system (or, more accurately, contact tracing systems).

Contact tracing: the Philippine experience

The World Health Organization (WHO) defines contact tracing as "the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission." It says the process involves five major steps: defining contacts, identifying contacts, informing contacts, managing and monitoring contacts daily, and data processes and analysis. It may be done either by people or through the use of digital tools. As regards the latter, the WHO warns that they "should not be considered as single solutions for contact tracing, but rather as complementary tools and should be carefully identified and analyzed for technical, cost, and ethical issues."

In the Philippines, contact tracing was immediately identified as a key public health intervention for COVID-19 response. According to Department of Health (DOH) Memorandum 2020-0189, the DOH Epidemiology Bureau is to provide the necessary guidelines and oversight for all contact tracing activities. It also includes instructions for the processing and disclosure of personal information of patients, although none of them are meant specifically for digital contact tracing tools. The DOH Memo also requires all government agencies involved in the effort to enter into a data sharing agreement with the DOH to ensure accountability over all collected information.

Soon after, through its Resolution No. 27, the Inter-Agency Task Force on Emerging Infectious Diseases (IATF-EID) adopted StaySafe.ph as the government's official "social-distancing, health-condition-reporting, and contact-tracing system". Developed by the private firm, MultiSys Technologies Corporation (MultiSys), it features QR code generation and scanning, and acts as a contactless and paperless digital logbook for establishments.

The endorsement immediately faced criticisms. Local IT experts raised privacy and security concerns, like the app's excessive permissions and unclear parameters on post-pandemic information use. Some wondered if the extensive citizen database it would entail will be used in relation to the 2022 elections or for targeting government critics.

Toronto-based thinktank, The Citizen Lab, seemed to corroborate those concerns when their technical analysis showed that StaySafe was collecting device geolocation data and storing it in an unsecure manner. Other dangerous permissions it was requesting for included the taking of photos and videos, as well as reading users' photos and other files. The group also flagged vulnerabilities it felt could be exploited to expose users' identities and health status. While MultiSys resolved most of these after it was notified, it continues to keep the app's source code and white paper under wraps, making third-party audits difficult, if not impossible.

In June 2020, the IATF-EID ordered MultiSys to transfer all information it had collected via the app to the DOH and migrate them into the DOH's Covid-Kaya system. It again referred to StaySafe as the government's contact tracing app of choice and urged all other existing contact tracing apps to integrate with it. The Task Force did warn MultiSys that its failure to comply with all requirements within 30 days would result in the withdrawal of the IATF endorsement.

Despite this, as of 21 January 2021, user data still remained with MultiSys. According to its CEO, the government still couldn't accept the data because it can't afford the necessary cloud storage services. As for the IATF, for some reason it still hadn't walked away from its endorsement. The other government-backed contact tracing systems are also still in use.

> "Some wondered if the extensive citizen database it would entail will be used in relation to the 2022 elections or for targeting government critics.

Public transit systems MRT and LRT have their own separate contact tracing apps (MRT-3 Trace and ikotMNL, respectively). And there is also TRAZE which was developed jointly by the Philippine Ports Authority and Cosmotech Philippines, Inc., for the purpose of monitoring the movement of people inside Philippine ports. As per the IATF-EID's Resolution No. 101, though, Traze is now to be integrated with the StaySafe system.

Many local government units (LGUs) also came up with their own digital contact tracing systems, either in the form of a mobile app or a browser-based tool. For instance, in January 2021, the city governments of Pasig, Valenzuela, and Antipolo forged an interconnectivity agreement to integrate their respective contact tracing solutions (PasigPass, ValTrace, and Antipolo Bantay Covid-19, respectively). Their mayors gave assurances that their systems have adequate safeguards, and are covered by a data sharing agreement, recognized under Republic Act 10173 (DPA), the country's data protection law. Mandaluyong joined the group in March with its MandaTrack app. Just like what happened to Traze, the IATF-EID also issued a resolution directing the use of StaySafe by LGUs. It reiterated such directive in January 2021, which meant, according to Presidential Spokesperson Harry Roque, that all LGUs that have their own contact tracing apps are already required to integrate their own systems with StaySafe.

As of this writing, it doesn't seem like that has happened. The country's contact tracing system is still in disarray. In March 2021, contact tracing czar Benjamin Magalong called the attention of lawmakers to the "deteriorating" state of the country's contact tracing. According to him, the contact tracing ratio has fallen to 1:3, which is far from the ideal of 1:30 to 1:37 in urban settings. When asked to explain the dismal performance, he gave the same oft-repeated refrain: lack of a uniform data collection tool among LGUs, non-use of contact tracing analytical tools by LGUs, and the continuing delay in the turnover and use of StaySafe.

It is interesting to note that the United States, in all its technological sophistication, also encountered the same problem with its own contact tracing efforts. Public health experts there suggested that a big part of the problem was the lack of coordination between the federal government and individual states. A glaring similarity with the local situation.

Ensuring secure and effective digital contact tracing

In February 2021, House Speaker, Lord Allan Velasco, filed House Resolution No. 1536, which urges the IATF-EID to establish a unified national contact tracing protocol. This would require the designation of a single government agency or body as the central repository of information. Velasco noted that the numerous apps currently in use and the decentralized approach to data storage has led to redundant products, cost duplication, and less effective solutions. The Resolution also brought attention to the poor interconnection and data sharing arrangements between solution providers and DOH's central database. To address these, the resolution calls for encrypted data transmission, a unified procedure for solution providers, compliance with the DPA, and real-time data access to accredited contact tracing app providers.

When the Resolution was taken up in a hearing, Eric Tayag, director of the Bureau of Local Health Development and the National Epidemiology Center, recommended that the DOH be the personal information controller for all health-related data. The DICT shall oversee the systems, while the DILG would be in charge of deploying the technologies. One thing that was not clarified was how the Resolution will be harmonized with the IATF's relevant directives.

The WHO has released several documents to serve as guidelines for the design and implementation of digital contact tracing tools specifically for COVID-19. One of the most instructive is an interim guidance released in May 2020, which identifies 17 principles that are designed to guide governments, health institutions, and private actors in the ethical and appropriate use of digital proximity tracking technologies to address COVID-19. Some of the principles are listed below and have been examined in the context of the StaySafe system:

1. **Testing and evaluation.** IATF Resolution No. 45 requires that the StaySafe app undergo necessary testing (e.g., penetration testing and vulnerability assessment), before the DICT and NPC certify that it is feasible for donation to the DOH.

2. **Use restriction.** This concern has been raised several times regarding StaySafe and other government contact tracing efforts. It's particularly relevant because most of the digital tools available today were developed in partnership with private companies that may want to use the collected data for their own purposes. The sale and use of data for commercial purposes or advertising activities should be strictly prohibited, albeit there are instances when this principle is not followed. In one of the contact-tracing apps used by an LGU, a pop-up message asks the user if they want to create an account with a certain bank after registration. There have also been reports of users, upon registration, receiving an SMS message from a certain group gearing up for the 2022 national elections.

3. **Voluntariness**. While it is unclear whether StaySafe will be made mandatory for all citizens, the required integration of all other contact tracing apps with the StaySafe system will effectively make it so.

4. **Transparency and explainability**. Information about data collection and processing shall be transparent and made available in clear, unambiguous, and accessible language. StaySafe has a rather lengthy Privacy Statement available in its website and in the app itself. It is good, though, that the Statement is organized, thereby making it easy to digest.

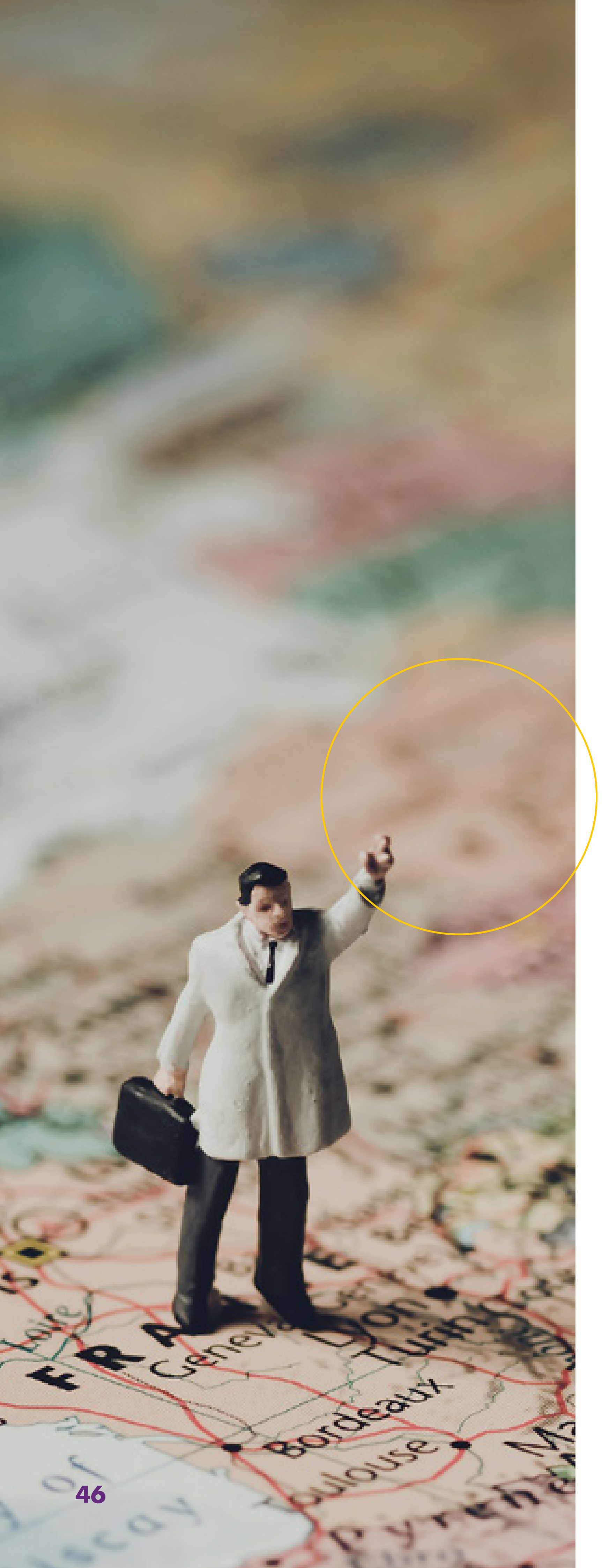
5. **Limited retention.** Data retention shall be limited to the period of the pandemic response, except for the purposes of research or epidemic planning, subject to appropriate regulation, oversight and informed consent, where required. According to Staysafe's Privacy Statement, it retains manual contact tracing data for 60 days, and digital logbook data for 30 days.

6. Infection reporting - Reporting into a digital proximity tracking app that a user has tested positive for COVID-19 could be done through several channels, such as a self-reporting mechanism. StaySafe uses this particular scheme.

7. **Accountability**. Individuals subjected to unwarranted surveillance must have access to effective remedies and mechanisms of contestation. Although contact tracing tools fall within the ambit of the DPA, it remains to be seen how the NPC is able to deal with complaints regarding the processing of personal information by such apps.

8. **Independent oversight**. The WHO recommends the establishment of an independent oversight body for both the public agencies and the private businesses that develop and operate the contact tracing apps. No such body has been established for StaySafe or any government contact tracing app.

9. **Civil society and public engagement.** As of April 2021, months after StaySafe was named as the Philippine government's official contact tracing tool, no public consultation has been held regarding the design and implementation of the system.



Other principles in the WHO guidance include time limitation, proportionality, data minimization, privacy-preserving data storage, security, notification, tracking of COVID-positive cases, and accuracy. Most of these are covered by the general principles of data protection. Unfortunately, until MultiSys, the DOH, or DILG make the white paper and the source code of StaySafe available to the public, independent actors will continue to find it difficult to examine the system's compliance with such principles. In the same vein, until an independent oversight body is established to keep an eye on all these things, the public would have to take the government's word when it claims it is actively protecting the privacy of the population.

Both are hard truths to swallow, but there is currently no plausible alternative. Given the way (i.e., passing the blame to one another) the concerned government agencies and even MultiSys itself have been dealing with multitude of concerns surrounding the current contact tracing system, transparency and accountability would appear to be the last thing in their minds.

This leaves the public with nothing except empty words and promises, and a practically non-existent contact tracing apparatus.

IATF-EID Resolutions re: StaySafe and digital contact tracing

Resolution No. 27 (April 22, 2020): IATF adopts StaySafe.ph as the official social-distancing, health-condition-reporting, and contact-tracing system that will assist in the government's response to COVID-19

Resolution No. 45 (June 10, 2020): IATF approves the recommendations of DICT and NPC:

1. DOH and Multisys shall enter into a deed or agreement regarding the donation and use of the StaySafe app, including the source code, all data, data ownership, and intellectual property.
2. DOH shall accept the app upon issuance by the DICT and NPC of a certification that the donation is technically feasible and secure, that systems are compatible, and that the arrangement is compliant with data privacy laws. The version of StaySafe to be donated to the DOH must be able to perform two (2) functions: first, for Bluetooth contact tracing that shall be connected to tracing technologies such as Google and Apple and second, as the frontend application system for LGUs.
3. The function to StaySafe shall be limited to data collection only, while all collected data shall be stored in DOH's Covid-Kaya system.
4. All data currently in the database of StaySafe shall be migrated to Covid-Kaya.
5. MultiSys shall comply with the above directives within 30 days from the date of the Resolution (June 10, 2020). Otherwise, the IATF's endorsement of StaySafe shall be withdrawn, and MultiSys shall migrate the data collected and stored in StaySafe to the DICT.

Resolution No. 85 (November 26, 2020):

1. Adoption and use of StaySafe by all national government agencies and instrumentalities, and LGUs is made mandatory. Its use by all other private establishments, facilities, and offices is also promoted. Those with existing contact tracing apps are enjoined to integrate their system with StaySafe.
2. All data collected through digital contact tracing apps shall be submitted to a centralized contact tracing data repository for integration and linkage with appropriate laboratory results.
3. The centralized contact tracing data repository shall be linked to either COVID-Kaya or the COVID-19 Document Repository System (CDRS), with all data submitted to FASSSTER (Feasibility Analysis of Syndromic Surveillance Using Spatio-Temporal Epidemiological Modeler For Early Detection of Diseases) for analytics and visualization.
4. The IATF Sub Technical Working Group on ICT Solutions shall formulate guidelines for the integration of digital contact tracing apps.

Resolution No. 87 (December 3, 2020): A Safety Seal Certification Program will be implemented for public and private establishments. Requirements to secure a Safety Seal include the adoption of the StaySafe app and the generation of its QR Code to be displayed in all entrances of an establishment.

Resolution No. 94 (January 14, 2021): The DILG is directed to ensure the proper enforcement of IATF Resolution No. 85 on the use of StaySafe by LGUs.

Resolution No. 101 (February 26, 2021):

1. The Safe, Swift, and Smart Passage (S-PaSS) Travel Management System of DOST shall be institutionalized as the one-stop-shop application/communication for travelers.
2. The StaySafe system shall be utilized as the primary contact tracing system. Traze App for airports, and such other existing contact tracing apps must be integrated with the StaySafe system.

A Tale of Two Systems

Maris Miranda

The public health crisis brought by the COVID-19 virus has managed to highlight varying governance strategies between countries. More than a year into this pandemic, it's become clear that some have fared significantly better than others–whether it's the overall government response or a specific area like contact tracing.

The New Zealand and the Philippine experiences are noteworthy contradictions. The former has earned praises for its overall pandemic response, including an efficient contact tracing system, that has allowed it to beat back the disease while protecting its economy. The Philippines, on the other hand, finds itself on the opposite side of the spectrum. More than a year since it began enforcing its infamous community lockdown, not only has the government failed to contain the pandemic, it has actually made things worse. Its contact tracing system? An abject failure.

What accounts for this stark difference? Plenty, apparently. While both claim to have a contact tracing mechanism as a key component of their respective pandemic response strategies, the similarities end there. There are the obvious differences in population size and wealth; but there's more to it than that. Some rich European countries have struggled too, while, China, which has the globe's biggest population, appears to have done well for itself, all things considered. A more nuanced comparison explains the contrasting fates of the two countries' contact tracing initiatives.

The first major difference pertains to the entities in charge of managing contact tracing in each country. New Zealand has its Ministry of Health (MoH) as the lead agency issuing guidelines, including limitations on the processing COVID-19 data. There are support agencies provide necessary assistance. Any Kiwi or NZ resident can easily find guides on the status of restrictions, what businesses can do despite the restrictions, how the contact tracing process works, and how establishments and public transport groups should collect visitors and employees' data for such purpose. All stakeholders are acting in concert, headed towards the same direction.

The Philippines, on the other hand, has an Inter-Agency Task Force for the Management of Emerging Infectious Diseases (IATF), which counts several government agencies among its members. With the Department of Health (DOH) as the lead, it issues nationwide guidelines and restrictions, while a National Task Force headed by the Department of National Defense (DND) implements said policies. In addition, sectoral agencies still release supplemental guidelines, supposedly to address policy gaps. Most, though, remain wanting, especially when it comes to data protection measures. The same may be said of local government units that also implement their own guidelines, further confusing the public. It's a mess, really.

> *More than a year since it began enforcing its infamous community lockdown, not only has the government failed to contain the pandemic, it has actually made things worse.* "

The data collection process is the second major differentiator. New Zealand's COVID Tracer, the national contact tracing app, does not need to collect user information in order to function. All data are optional and will be saved only on the device. Sharing is initiated by users, when necessary. Establishments manually collecting data are required to obtain the same set of information: name, time and data of collection and phone number. Those with a ticketing system (e.g., airlines, inter-city buses) are not required to collect data anymore since they already have the necessary information.

In the Philippines, there is no single prescribed dataset for collection. StaySafe.PH–the so-called official contact tracing app–collects its users' mobile number and health declaration checklist upon account creation. Using one's Facebook account to register is also an option. Meanwhile, various government agencies collect different sets of information for contact tracing purposes. The LTFRB requires public utility vehicles (PUVs) to maintain a passenger manifest but initially failed to identify what information had to be collected. It took another month before it came out with an issuance that informed public utility jeepneys (PUJ), at least, what they're supposed to gather. The Maritime Industry Authority added more data fields to its standard passenger manifest, like travel history and emergency contact details. Meanwhile, a joint issuance by the Department of Trade and Industry and the Department of Labor and Employement requires establishments and workplaces to collect health declaration forms from employees and contact tracing forms from visitors. Others like the Civil Aviation Authority of the Philippines have developed and use their own app for data collection.

Speaking of apps, use of the NZ COVID Tracer remains optional. Those who end up using it are informed that the app stores data on their device and automatically deletes the same after a specified period. Establishments may still collect data manually, but they must encode the data in a registry. For them and other contact tracing apps, the Ministry of Business, Innovation, and Employment prescribes a thirty (30) day retention period.

Filipinos have a more complicated system to deal with. The government requires the use of StaySafe.PH, but then allows the use of other apps, as long as they are integrated with it or are connected to the central database maintained by DOH. Many establishments opted to use their own apps, but without any integration plan. Others like the public transport sector were content with manual collection due to technological capacity issues. This means one person may need to download several apps and/or fill out multiple forms in a day in order to go about his or her daily routine. At this point, no one knows yet how well data collection is being implemented (if at all) by PUVs. In terms of data retention, StaySafe.PH also deletes collected data after a specified period. However, it is unclear if some details like storage location and whether any of the data supposedly being deleted are in fact kept on record. No explicit retention period has been given to those in the public transport sector.

All these differences are further reinforced by the way each country approaches privacy and security, and the range of concerns it is faced with. In New Zealand, the MoH uses Apple and Google's contact tracing framework for its app. It anonymizes users' identity and, as noted earlier, stores data only on the user's device. Users decide whether or not they wish to notify others anonymously if they should later test positive for the virus. The government also made it clear from the beginning that contact tracing data will not be used for any other purpose. It also shared the source code of the app as a transparency measure. At the same time, the Privacy Commissioner consistently voices out data privacy concerns even if it means going against the government's official position. His Office's website also has a page dedicated to any or all privacy concerns relating to the pandemic. Still, all these do not make a 100% secure contact tracing system. There have still been occasional mishaps along the way. The security of manually collected data, in particular, is harder to manage since businesses have varying capacities to collect, process and secure any information they collect. One cannot also avoid having one or two employees going rogue and violating existing protocols.

Those problems, though, are nowhere near the kind the Philippines has had this past year. With StaySafe.PH, red flags were observed almost as soon as it was endorsed by the government. There were issues relating to its features, compatibility with 2G devices, and default data retention policy. To date, its formal turnover to the government has yet to be finalized, for reasons that are confusing as they are numerous. There have also been reports of unauthorized use of manually collected contact tracing data, like the way they have facilitated the proliferation of unsolicited SMS. Also, as in the case of New Zealand, many Philippine establishments have a limited capacity to collect and protect the data they collect. Given these, it is doubly tragic that the country's data privacy regime just happens to be not mature enough to be able to respond effectively and consistently to prevailing issues. Most of the time, data privacy is seen as a hindrance rather than an enabler of pandemic response. Some business groups have even called for the suspension of the data protection law supposedly to make contact tracing easier. There was a time when even the IATF required the disclosure of patients' identities for the same purpose. As far as the privacy regulator itself is concerned, the National Privacy Commission (NPC) has publicly dismissed the proposal to suspend the Data Privacy Act. It also voices out its opinions regularly, albeit they have taken a more conservative stance in relation to most issues (e.g., non-compliance by StaySafe.PH with data privacy regulations). In fact, the agency even released a policy during the pandemic making it easier for entities to share personal data.

Taken together, all these notable differences would explain the different levels of trust the population of the two countries ascribe to their respective contact tracing systems. This is crucial because many tend to gauge the success of a pandemic response solely through economics and forget that it is also a social issue that hinges on trust.

With contact tracing, everyone has to understand that it is a task that requires skill—specifically, medical skills—and the ability to locate people who may end up refusing testing or treatment. It is more than just knowing where to look and who to look for. It is also about being trustworthy in the eyes of the people.

If one takes a look at the Kiwi experience, it is evident that people there were initially hesitant and unconvinced too of their government's initiatives. Some patients became more confused when contact tracers managed to speak to them, and there were also reports of biased arrests in relation to their own community lockdowns. It took some time, but eventually public trust surged because the government eventually got it right. Proper information dissemination played a key role. As a final testament to the effectiveness of their strategy, the Prime Minister got re-elected because of the leadership she had shown during the pandemic.

In the Philippines's case, one study shows that the government's pandemic response got the highest disapproval rating in Southeast Asia. And nobody was the least bit surprised. The country's contact tracing system alone is already a disaster. Contact tracing teams are still undermanned and under-resourced. The pandemic response continues to revolve around the police and the military, notwithstanding all the flak this strategy has gotten for its obvious flaw. And this is after the government has already had a year to figure things out. The misinformation, disinformation and false claims that continue to proliferate have also caused more division in an already polarized atmosphere.

Learning the Kiwi Way

While New Zealand's contact tracing experience is not perfect, it has been effective in supporting the country's overall COVID-19 response. What has made this possible is the government's appreciation of the fact that the pandemic calls for a rights-based, health and scientific response. With a strong yet empathetic leadership at the helm, everyone went with the program and helped make the country one of the success stories to come out of this pandemic.

With arguably less resources at its disposal, the Philippines has a lot of things to learn from its Asia-Pacific neighbour. The government needs to be wiser and more efficient in its initiatives, particularly with contact tracing. A significant but necessary shift would involve getting more health experts in leadership positions and having more transparency in all efforts. The IATF should then issue clear guidelines that cover both manual and digital systems. Data protection should be embedded in those rules. Data requirements should also be uniform.

The NPC, as the country's data protection authority, has to be more assertive with its mandate, as is expected from an independent government body. Its general and frequently vague statements will do no good. People and organizations need clear and concrete rules to adhere to. This may very well be the biggest test to its mandate since it was established five years ago.

On one occasion, the Philippine government has had the opportunity to distance itself from a comparison with its Kiwi counterpart by claiming the comparison is unfair. It noted that New Zealand is a smaller and, at the same time, wealthier country. In the greater scheme of things, it is that excuse that is unwarranted. The New Zealand government succeeded and continues to do so because of the mutual trust it observes with its people. It achieved that level of trust by introducing measures that produced good results without compromising the people's rights. Now if only the Philippines can do the same.

The Doctor is Online: Telehealth in Times of Crisis

Ivy Patdu

The pandemic of this century has transformed our everyday lives. Physicians, nurses and other healthcare workers at the frontline risk their lives to save others while fearing collapse of the health system. The issues are not just about available hospital beds but whether there are enough healthcare professionals to take care of patients and whether there are enough oxygen and medicine for those who are sick. People experienced wave after wave of reported cases and the government imposed community quarantines to slow down the curve. The medical community at one point called for a lockdown because the "healthcare system has been overwhelmed."

Faced with this health crisis and with the general population's restricted movements, access to healthcare became a challenge. While resources and manpower were dedicated to manage COVID patients with severe disease, there remains many other patients with medical conditions requiring attention. People were, however, discouraged from seeking out-patient consults unless necessary. Appointments with physicians were limited and scheduled to follow safety protocols because it was a health risk to have many waiting patients in clinics. In order to provide access to healthcare while limiting exposure to possible infections of both the patient and the physician, telehealth became a viable alternative.

The World Medical Association defines telemedicine as the "practice of medicine over a distance in which interventions, diagnostic and treatment decisions and recommendations are based on data, documents and other

information transmitted through telecommunication systems." While "telehealth" and "telemedicine" are often interchanged, telehealth is a much broader term, referring to the provision of all aspects of healthcare, including health promotion.

The initiatives for telehealth in the Philippines started long before the pandemic. It is part of the broader initiatives for e-Health and is included in the Philippine's National Objectives for Health. The University of the Philippines National Telehealth Center has in place a telehealth program which provides telehealth services, primarily in geographically isolated and disadvantaged areas. A doctor-to-the-barrio for instance is able to consult with a specialist usually located in the Philippine General Hospital through Information and Communications technology (ICT)– cell phones, electronic mails and other technology platforms. There are also telemedicine providers in the private sector providing services within affiliated institutions or as part of direct to consumer services, among various arrangements. The pandemic, however, fast-tracked the use of telehealth in providing care.

The most commonly used mode of telehealth during the pandemic is through a virtual consultation between a patient and a physician. The Department of Health entered into partnerships with private companies and local government to allow the public to use hotlines or platforms to get medical advice. Physicians also started making themselves available online for consultations. Patients were encouraged to consult through telehealth before scheduling a face-to-face consult, if still necessary.

Typically, a patient may sign up for a dedicated telehealth platform to set appointments with physicians. They may also contact a healthcare provider directly through a messaging or video-conferencing platform. Patients will be asked to provide their personal information when using these platforms, and to agree with rigid terms of use. During the virtual consult, they will be asked to share very sensitive information to a physician at a distance, or to direct the phone camera to parts of their body as part of the medical examination. Another person may also be asked to assist the patient and sit-in during the consultation. The patient may also be asked to send a laboratory result to a physician or receive a prescription or medical abstract online. The interaction necessarily involves processing of health information. The physician-patient relationship is founded on trust and this is particularly important in telehealth.

The acceptance of this new mode of delivering healthcare is not without challenges, considering that it is a relatively new experience for many patients and physicians. Concerns have been raised on privacy and data security involved in a teleconsultation. Many physicians were reluctant to practice telemedicine because of fear of violating existing regulations. In the United States, the Office of Civil Rights, announced that it will not impose penalties for noncompliance with the regulatory requirements under the Health Insurance Portability and Accountability Act (HIPAA) "for good faith provision of telehealth during the COVID-19 nationwide public health emergency." No similar notice was made in the Philippines, though there were sectors calling for the suspension of the Data Privacy Act for purposes of contact tracing.

Instead, the Department of Health with the National Privacy Commission issued a joint memorandum circular, "Guidance on the Use of Telemedicine in COVID-19 Response" which was intended "to enable patients to receive health services while staying at home" and also "to avail of COVID-19-related services." The Circular incorporates policies for data collection for contact tracing and care coordination for COVID-19 patients. The Circular also provided requirements such as an informed consent for telemedicine practice, and obligations for data protection on healthcare providers. Implicitly, the Circular attempts to allay concerns on data privacy. Subsequently, the Department of Health with the University of the Philippines Manila issued another circular on "Telemedicine Practice Guidelines" providing specific recommendations for synchronous virtual consults to patients. These issuances are complemented by Food and Drug Administration (FDA) guidelines covering electronic prescriptions for the benefit of individuals vulnerable to Covid-19.

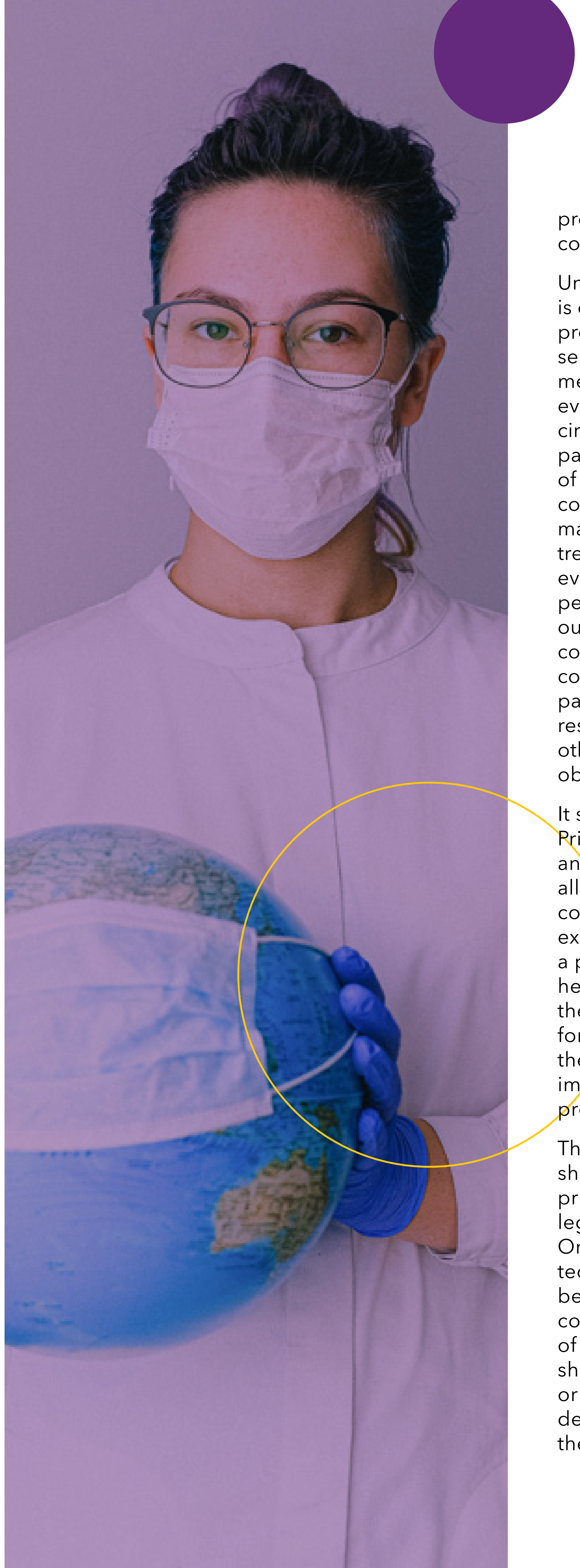
The use of ICTs in health requires considerations of possible risks. In one study which reviewed articles relevant to patient safety risks associated with telecare, concerns centered on the limitations presented by the use of ICT as opposed to traditional face-to-face care, the lack of understanding of telecare services for both patient and staff, and technical aspects like integration with existing systems and usability of technology. Data privacy and data security are also important aspects in the implementation of telehealth services.

For patients, there were those who were uncomfortable with the idea that they are not able to see a physician face-to-face. Will the session be recorded? Who else can hear or see the consultation? Are messaging applications safe platforms to exchange information? These concerns are similar to the results of 2017 study where patients acknowledged the benefits of a video consultation but expressed concerns on "privacy, including the potential for work colleagues to overhear conversations, and questions about the ability of the clinician to perform an adequate physical examination. [Powell, 2017]"

Indeed, there are lots of issues that need to be addressed in Telemedicine, because it has not been fully institutionalized as an integral component of the health care delivery system in the Philippines. Necessity required adoption of telehealth even as questions remained on what standards to follow, whether the public has the technological know-how to seek a telehealth consult, and whether the healthcare professionals have been capacitated to ensure personal data protection when processing sensitive personal information. Privacy concerns will not be addressed by asking for exemption from laws from data privacy regulations. Telehealth has to be done right for it to be sustainable. Doing it right means ensuring that data privacy is not set aside for convenience.

Telehealth requires transparency. Patients should understand the benefits, potential risks and limitations of telehealth. In the same way that privacy notices are required when using applications or web-based platforms, the same information should be readily accessible to patients. Often times, patients readily send their laboratory results and other health information through messaging applications. Data security is not their concern. Healthcare providers should include these information when communicating with patients and provide them an alternative means of transmitting information. In general, patients should understand how their information is being processed, who has access to their records and the risks entailed by their chosen medium of communication.

For patients, agreeing to receive healthcare through telehealth should proceed from an informed choice. Consent is a common recommendation in telehealth guidelines in many jurisdictions. Consent is obtained for purposes of using telehealth as a means to provide healthcare, and for the processing of health information, where consent is the basis of processing.



Under the Data Privacy Act, consent is only one of the criteria for lawful processing of personal data, including sensitive personal information. This means that processing may be allowed even without consent under certain circumstances. For example, creating a patient medical record for management of patient generally does not require consent. The basis of processing may be the processing for medical treatment purpose, considered lawful even without consent. In cases where personal information will be used outside medical treatment purpose, consent may be required. For instance, consent is generally necessary if patient's health data will be used for research, marketing, educational and other purpose. Consent should also be obtained for video and audio recording.

It should be emphasized that Data Privacy is not limited to transparency and consent requirements but requires all aspects of data protection. Ensuring confidentiality, safety or security of the exchanged information in telehealth is a positive obligation on the part of the healthcare provider. In the Philippines, there are already existing guidelines for data privacy, primarily covered by the Data Privacy Act, a general law that imposes obligations on those who process personal data.

Those who process personal data should adhere to data privacy principles such as transparency, legitimate purpose and proportionality. Organizational, physical and technical security measures should be implemented to maintain confidentiality integrity and availability of data. This means that Personal data should be protected from unauthorized or unlawful processing, changes, destruction or loss of data. How will they store the patient data? Are the devices they use secure? Do they store and transmit health records in an encrypted form? Who has access to patient records? How will the physician deal with an interrupted connection? The rights of patients as data subjects should also be an important consideration, whether it is their right to adequate information relevant to processing involving health information, or their rights to have access to their records and to have them corrected if necessary.

Once a physician decides to practice telehealth, he or she should take the time to ensure that processes are in place to meet data privacy obligations. These obligations extend to any other person involved in the management of the patient or the processing of patient information, or those processing information on behalf of the physician.

In truth, these obligations apply to the practice of medicine, whether face-to-face consultations or telehealth. The physician by collecting and using patient information will have obligations for data protection regardless of the mode of delivery of care. The additional responsibility when practicing telehealth that needs consideration is the use of platforms for teleconsultations or for the exchange or storage of information. Under the DPA, the healthcare provider will have an obligation to use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. In practical terms, this means the physicians themselves should evaluate a platform before engaging its services. They should go beyond understanding the features but should ask questions on the security measures being implemented by the platform and any other means to demonstrate compliance with existing data privacy regulations.

On the other hand, efforts should be directed to empowering patients so that they can make informed choices about telehealth. The patient's fears should be addressed to make telehealth an acceptable option. Data Privacy should be considered an important component of the telehealth practice to enable patients to trust the physician and the system. Privacy concerns should not be one of the reasons why patients hesitate to seek teleconsultations, particularly at this time, where medicine at a distance may be the safest alternative.

Patients should understand that telemedicine may not be appropriate in all cases and they may still be asked to go to the hospital or clinic, or requested to do additional diagnostic examinations. Where appropriate, a telemedicine consult means that patients may be able to receive medical attention while at home. They will avoid the travel to the hospital and minimize their possible exposure to infection. They will be spared the waiting time in the doctor's clinic and they may have the assistance of their family members during the consultation. At the same time, telehealth allows the hospital and limited manpower to be directed towards patients most in need of a face-to-face consultation. These benefits can be realized if the patient is well-prepared for a teleconsultation. While healthcare providers have data privacy obligations, the patient should take steps to maximize a teleconsultation *(see below)*.

The benefits of telehealth is not limited to times of health crisis and should be acknowledged for its potential to make quality health care more accessible to the people. In the Philippines, before the pandemic, the Philippine Statistics Authority said that six out of ten deaths are not medically attended. There are geographically isolated and disadvantaged areas where a community may even need to travel by boat to reach a hospital. It has been reported that the doctor to population ratio in the country is 0.4:1000 with only 40,775 medical doctors for a population of more than a hundred million. Given these realities, telemedicine should not be viewed as a temporary solution but a means of filling in the gaps of a fragmented healthcare system. Privacy concerns and minimizing the risks for patients should be part of these initiatives to make telehealth sustainable and acceptable.

Tips for Maximizing Your TELECONSULTATION

1 **The patient should take time to understand the process of consulting online.** If asked to sign up with a telemedicine platform, patients should look up the privacy notice and read the terms of conditions. Where the consultation is done through messaging applications and video conferencing platforms, the patient should be careful in sending medical records and wait for instructions of the physicians. Patients should remember that they also have a responsibility in protecting their personal information.

2 **Patients should prepare the information that will most likely be asked by the physician in order to make the most of the consultation.** Physicians will usually ask about what the patient is feeling, how his or her condition progressed over time, and what other medications are being taken. The patient should be truthful in disclosing information. The information will help the physician evaluate and manage the patient's condition. Accurate and complete information can help save lives.

3 **The patient should ensure good internet connection, and decide what device he or she will be using for the consult.** Patients should also choose a quiet place conducive to good communication and where interruptions would be unlikely. In case the teleconsultation is not completed, the patient should be ready to go to a clinic or hospital for urgent concerns.

4 **The patient should decide on whether he or she needs to be accompanied by another person during the consultation.** The physician may also be the one requesting that the patient be accompanied, especially if the examination being done online requires assistance from another person.

5 **The patient should not hesitate to clarify with the physician any information about instructions given, prescriptions provided, or any other doctor's order.** Patients can also list down beforehand questions that they may have for the physician.

Protecting Children Online

Ivy Patdu

The pandemic has normalized the child's online presence. The imposition of quarantine measures means many people are confined in their homes, having had to adapt quickly to a largely digital lifestyle. The pandemic is the single biggest disruption that has fast-tracked digital transformation. Unfortunately, it also has drawbacks in terms of child safety. Children have been spending a lot of time online, whether for purposes of school, entertainment, and other social interactions. Being at home is probably the safest thing for them at this time, and parents might be less worried for their kids. The time children spend online, however, is not without risks.

What could possibly go wrong?

If parents have not even considered this question, then we truly have a problem. We have become so used to the online environment, especially social media, that we may have conveniently forgotten its dark side.   The ease by which personal information can be transmitted online—be it the transmission of photographs or real-time virtual interactions—contributes to its misuse or abuse. There is also the anonymity afforded by the internet, which is a double-edged sword. It protects freedom of speech and internet freedom but it may also be used to propagate harassment and other criminal activities. Against this backdrop, children could have unrestricted access to the internet, engaging in unmonitored activities, and developing relationships with online "friends". A child may simply click a button that says "I'm over 18" to access inappropriate content, or create multiple profiles to override age restrictions.

On one end, we have child pornography. Pre-pandemic, the proliferation of online child pornography was already a problem, perpetrated by adults taking advantage of internet access and the ease of digital transactions. While the country has been in lockdown since last year, authorities have observed an increase in cases of online sexual exploitation of minors. They include instances where a close relative or parents themselves send pictures of children in compromising positions or engaged in sexual acts in exchange for money. Very little value is placed on privacy, in general, with children's rights often overlooked.

There are also cases where children themselves use social media to put themselves in situations where they can be exploited. In a study on the "Commercial Sexual Exploitation of Children in Metro Manila in the digital age," children aged 13 to 18 were interviewed and 66 percent admitted having made online transactions (of a sexual nature) to get customers, where some teens "play the role of a pimp for their peers but would also be a sex provider at the same time…" The report stated that "some of those who pose and mime sexual acts in front of cameras believe that the abuse is less because there is no physical contact."

Stories of predators lurking online are not even new. Yet we all seem to need constant reminders about the dangers of cyberspace. In efforts to identify online predators, a Dutch children's charity set up a fake profile of a 10-year-old Filipino girl, using a realistic computer avatar, and named her "Sweetie." They then entered chatrooms where she was swarmed with male attention almost immediately. After ten weeks, a total of about 20,000 men had contacted her, a thousand of them having offered her money to take her clothes off. "Sweetie" is a wake-up call to the risks that a child may encounter when navigating the online world.

Today's children were born in an already digitally connected world. It's relatively easy for them to appreciate the possibilities of technology. At the same time, we have been quick to allow them access to the web but too slow in ensuring their protection. While there are certainly laws that criminalize child online sexual exploitation and child abuse, there remain gaps in the regulation of children's online activities. For instance, most children view social media in wholesome light, oblivious to its characterization as a "stalker's paradise" and unaware of risks their information are exposed to.

Certainly, the internet, in general, is a medium for entertainment and even a healthy dose of personal publicity. Children get to play online games where they meet and interact with other players. They have access to messaging applications, as well as social media platforms where they get to connect with friends. A friend of a friend may be welcomed to a child's online social circle but a social media "friend" could be anyone, including creeps and posers. Back in 2002, 13-year-old Alicia Kozakiewicz of Pittsburg, Pennsylvania, met someone online who "seemed nice" and whom she thought to be a boy her own age. He turned out to be a 38-year-old pedophile who ended up kidnapping her. Her experience made Kozakiewicz an advocate for internet safety and the protection of children online. After her rescue, the "Alicia's Law" was set up, which assured funding for the Internet Crimes Against Children (ICAC) Task Forces.

The internet is a place where children freely share information about themselves. While they claim to also care about their privacy, it has yet to translate to their online activities. This is the observed privacy paradox, which is actually not limited to children but cuts across ages. In one of the cases decided by the Philippine Supreme Court, the issue revolved around the posting by students of sexy photos on Facebook which became the basis for their Catholic school to bar them from their graduation ceremonies. While the case is notable because of the Court's discussions on the reasonable expectation of privacy in online social networks, it also provided insights on how children use social media and the types of information about themselves they post online. The case of a student who uploaded nude photos of his ex-girlfriend in a porn website after they broke up is another example showing how the Internet is used to propagate inappropriate and even illegal acts. In their online activities or when disclosing information about themselves, children may not be thinking of the fact that their acts could be digitally recorded, or that their information may be used for unauthorized purposes, or their photos published elsewhere.

Sometimes, parents themselves may overshare their child's sensitive information online, seemingly unaware of the dangers they are inviting. A Forbes article coined the term "sharenting" and claims that parents are the biggest violators of their own children's privacy. Indeed, sharing a child's name, birthdate, and geotagged photos could lead to identity fraud in the future because bad actors could already be storing this information. The pictures alone could already end up on a child pornography site. The article also expressed concern for the possibility that children's data shared today could be used to make decisions about them in the future. For instance, will these be used to evaluate their university application and insurance costs?

Compounding today's threat to online child safety was the cybersecurity issues sustained last year by different sectors that cater to youngsters, including the data breaches of several universities. While the rapid shift to online education during the pandemic was generally commendable, it cannot be denied that it invariably exposed young students to increased privacy risks—from the collection and transmission of their personal information, to the security of learning management systems. Even platforms used for online meetings and virtual classes have been subject to hacking.

> Very little value is placed on privacy, in general, with children's rights often overlooked. ”

Finally, there are also those risks inherent in the collection of children's information by third-party platforms. For instance, security concerns have hounded Internet connected-toys, including one case where personal information about customers, including children's voice recordings, were stored in an exposed database. There was also a doll that had smart conversations with kids, and which ended up getting banned in Germany where it was considered an illegal espionage device. Content platforms and other online applications may also be collecting and using information about children. In 2019, the FTC imposed a penalty on Google and YouTube for collecting personal information about children and using cookies to track their online activity without complying with the notice and consent requirements of the US Children's Online Privacy Protection Act.

Are laws sufficient to protect children online?

According to the European Union's General Data Protection Regulation (GDPR), "[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user-profiles and the collection of personal data with regard to children when using services offered directly to a child…"

With that, there is at least an acknowledgement that children are considered a vulnerable segment of any population. However, while laws criminalizing child pornography and other forms of child exploitation could act as deterrents, more often than not they address these problems after the fact. They do not specifically address child protection, especially in the online context. They do not impose obligations on those who allow children to create online profiles or those who offer content accessible to children. Some jurisdictions like the EU and the United States do, but we have yet to see similar laws in other countries.

There are also differences between existing regulations. For instance, they sometimes differ in the way they define a "child" for purposes of being included in their scope of application. The GDPR provides that "in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Otherwise, such processing shall be lawful only if and to the extent that consent is given by the holder of parental responsibility over the child." However, the GDPR allows Member States to provide a lower age threshold as long as it is not below 13 years old. Meanwhile, under the US Children's Online Privacy Protection Rule, a child is someone under the age of 13.

Here in the Philippines, there is still no law that governs children's internet use. The general definition of a child is a "person below eighteen (18) years of age or those over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation or discrimination because of a physical or mental disability or condition." In general, a minor who has not turned 18 cannot give consent to a contract. There are, however, no precedents to show attempts to regulate children's online activity including the use of information society services, or to formally question whether minors creating online accounts is, by itself, a valid legal act under current laws.

There is an initiative to cover child online protection in the recent bills to amend the Data Privacy Act of the Philippines. The proposed law states that one of the conditions for processing personal information lawfully, in the case of information society providers offering services directly to a child, is consent of the child who is over 15. For younger children, the processing will be lawful only if consent is given or authorized by persons exercising parental authority over them. During discussions of the said bill in Congress, there was a debate on the appropriate age where parental consent is required, with invited stakeholders expressing varying views. Representatives from Facebook and Google, for example, argued that the age should be lower based on the benefits of internet access to children. Children's rights advocates, on the other hand, propose a higher age based on perceived risks to child safety.

If the amendment to the DPA is passed, this will be a first step towards laying down rules for children's online privacy protection. Afterwards, the greater challenge will be about implementation and effective regulation.

What we can do for now

The Internet is not always a safe place, especially for children. What has become clearer since last year is that we are living in extraordinary times when the issue of online child safety deserves more of our attention. Children cannot be denied the use of internet-connected gadgets because of the latter's potential benefits, emphasized by quarantine-related needs. On the surface, children seem pretty safe inside the home, but a child online wades in murky waters, exposed to diverse risks.

The impact of our online activities on personal privacy, how we can exercise control over the processing of our information, and how we can protect children should be a priority. Government plays a part in establishing and strengthening this framework but it may take a while before the regulations are fully implemented. As data subjects and technology consumers, there are already steps we can take to safeguard our children.

As a community, we should take steps to empower our children with the knowledge, skills, and tools to safely navigate the online world. This entails a continuous effort to make them understand the risks that attend their use of the internet. We can start by cultivating in them an appreciation of the value of personal information and by giving them specific guidance on what they can do to protect their own privacy—from being cautious about information shared online, to understanding security features and privacy settings of their smart devices. We must advice them to be careful and even skeptical, not just when interacting with other people online, but also when downloading and using applications or clicking on links.

Parents should also take the time to reasonably monitor and regulate children's online activities. It is important to set boundaries while ensuring that children can freely communicate with a trusted, responsible adult. In the end, the internet that connects people online should not be a reason for families to grow apart or for parents to be less involved in their children's lives.

Doxing and the right to be "let alone" in the Digital Age

Ivy Patdu

We live in what has been coined as the fourth Industrial Revolution– blockchains, the internet of everything, and artificial intelligence, among others. Volumes of data are being analyzed to create meaningful information at a pace beyond that we are able to imagine. The combined power of information and technology is transforming our everyday lives. To borrow from Charles Dicken's opening lines in a "Tale of Two Cities," we are in the best of times and the worst of times.

The internet makes information available in an instant, but it has also paved the way for misinformation and disinformation. Technology connects people across the globe but it has also meant the rise of new species of crimes. We have become familiar with terms like "cyberbullying" and "cyberlibel". Today, people can easily have their 15 minutes of fame. Unfortunately, it also means a single moment of weakness can become etched in the internet that almost never forgets.

Imagine your own digital footprint. What information about you is found online? Try searching for your name in one of the search platforms. Your address, phone number, photos and social media profiles may all be publicly accessible. They may be information you shared voluntarily, or information about you published by other people. There are also those information about you that are not readily visible but are being collected nonetheless, like your browsing history, your mobile device, or your location. How will all this affect you now and in the future? Will information about you be used to make decisions that may significantly impact your life? Are you still able to exercise control over how your information is used?

According to one social media survey, 70% of employers may consider social media profiles in evaluating potential employees. There have also been reports of visa applications requesting social media identifiers. Finding information about someone has become easier. With just a few clicks on your mobile phone, you get to see a person's key personal and professional details. This kind of accessible information is useful and even desirable when it works to the advantage of a person. When taken out of context and used maliciously, however, those same personal details could be used to make you the target of ridicule, harassment, blackmail, and more.

Imagine, for instance, your photos becoming used in social media memes, or you suddenly receiving threatening private messages because of your political belief, profession, or gender. Posts in Facebook of sleeping healthcare professionals became viral with some netizens criticizing them for "sleeping on the job". These are the realities of social media today.

The malicious use of personal data is known as "doxing", and yes, this is a cause for concern, because virtually everyone can be a victim–including those who think they have very little online presence. If a perpetrator is determined and resourceful enough, he or she can dig up enough sensitive information about a person, make them publicly available online, and expose that person to all sorts of ridicule and harassment. Worse, even information about relatives and friends of the actual target are sometimes included in the revelations.

At the height of the pandemic panic last year, some netizens went double time with doxing, publicly naming and shaming alleged COVID-positive individuals. Netizens exposed their faces on social media and showed photos of where they went and who they socialized with. Those people were called names for being "irresponsible." The perpetrators seemed unaware that their doxing activities were just as irresponsible.

Doxing (sometimes spelled "doxing") came out in the early days of the Internet, at a time when users used pseudonyms or aliases when online. The term is derived from the phrase "document tracing" and "dropping docs" on someone—a revenge tactic of hackers carried out by unmasking the real-world identity of a targeted individual. In the era of social media, when users rarely want full anonymity but still desire some degree privacy, doxing has come to mean as "the act of finding or publishing private information about someone on the internet without their permission, especially in a way that reveals their name, address." An article in CSO Online concisely defines doxing as "the act of weaponizing personal information," hinting at its highly unethical nature.

Today, perpetrators of doxing may still hide in anonymity to avoid reprisal and possible legal troubles. But there are those who openly do it, unaware that there is even a technical term for it. They are motivated by a sense of social media activism, believing that what they are doing is beneficial or at least morally justified. They feel they are within their rights to bring to the public attention what they consider to be unacceptable behavior. If some people come forward and claim that it already qualifies as cyberbullying, they defend themselves by arguing it is not bullying if the target "deserves" it enough.

Take the case of a lawyer who earned the netizens' disdain and found herself isolated in the eye of a social media storm when a post of her encounter with a traffic enforcer went viral. People dug up her personal life, curated them, and then republished them online, exposed to widespread criticism. A similar fate was endured by a physician called out for allegedly refusing to provide treatment to a patient. Feeling aggrieved, a patient aired grievances online. The post went viral, attracting netizens from all over to scorn the physician. Some culled photos and other personal details from her past social media posts, and fed these back to an engaged and enraged public. The physician suddenly found herself a prejudged respondent in a trial by social media, wherein one cannot appeal for balance or fairness. Even the website of the hospital she worked in became a target for hackers.

When a post accusing someone of some wrongdoing goes viral, people who see it often feel emotionally compelled to express their frustrations and/or to make a stand, especially when it relates to an issue they strongly feel about. They think it's only right to ask for accountability, albeit in the form of public shaming. Some, in particular, feel it is a valid exercise of their right to freedom of expression and of free speech. The issue is a matter of public concern, they would say, and the sources of information are publicly accessible anyway. Indeed, had it not for the accessibility and availability of technology and social media, the public would not have known of how a policeman shot two people point-blank, or how an African-American died while being restrained by law enforcement agents. Do these cases not involve the disclosure of personal information done in the service of citizen vigilance?

> ***While social media vigilance has its democratizing and empowering bright spots, we must never turn a blind eye to the fact that it is also open to abuse. Freedoms are not absolute.*** "

While social media vigilance has its democratizing and empowering bright spots, we must never turn a blind eye to the fact that it is also open to abuse. Freedoms are not absolute. One's rights may be limited when it infringes on those of others. In doxing, for instance, where a post may be viewed by thousands of people in a few seconds, consequences may be difficult to reverse. Netizens may easily jump to conclusions based on a one-sided but emotionally persuasive content. Its large and ever-increasing number of likes and shares would even be taken as "proof" of its legitimacy. Instead of fact-checking, people are inclined to take a short-cut and just assume that if a news organization or someone they respect or admire has shared it, then it must be true and ought to shared further in the spirit of social involvement. How many will take the time to verify information or get the complete story before forming an opinion?

Meanwhile, victims of doxing rarely find it easy to obtain remedies for the privacy violations or ruined lives or reputations they will have to endure as outcomes. The anonymity and accessibility made possible by the internet, and the lack of speedy processes for complaints involving

cyberlibel or cyberbullying certainly do not do them any favors.

Are there possible remedies that can be explored under data protection laws? It's hard to say, too. In a recent advisory opinion from the National Privacy Commission (NPC), the complainant inquired on whether a case can be filed against a person who took an intimate photo of the complainant with a partner while dining in a restaurant. This photo was afterwards uploaded in social media with a derisive caption. The opinion stated that the "protection of the right to privacy extends to public spaces and information that is publicly available," citing a United Nations High Commissioner for Human Rights report. Unfortunately, the report focused on the digital surveillance, monitoring, or data collection by the State or business enterprises, and it did not include discussions on how the privacy rights of individuals in public spaces will be reconciled with general claims of freedom of expression by individuals. Thus, a lot of questions still remain. Will the same principles espoused by the report apply when an individual takes a photograph of a public space that may include individuals? Will a person be liable for making a commentary on matters of public interest involving publicly available information?

The NPC advisory opinion suggests that secretly taking photographs of people, even in a public space, and subsequently posting them online, may be considered unauthorized processing, depending on the circumstances. The surrounding facts will have to be considered. It effectively says that it may be possible for the affected individual to exercise his or her rights as a data subject, such as asking for the blocking removal or destruction of his or her personal information, upon substantial proof that it was unlawfully obtained or used for unauthorized purpose.

This advisory opinion is in line with the right to be forgotten of the European's General Data Protection Regulation (GDPR). This right remains to be challenged, particularly with regard to the responsibility of search engines to remove access to online content that are prejudicial to data subjects. The Court of Justice of the European Union has upheld the right as claimed against a search engine, but limited its application to the Union.

Other than advisory opinions from the NPC, there has be no case law exploring the right to be forgotten under the Philippine's Data Privacy Act (DPA). The law is clear though that it is a right that may be demanded from a person who collects and posts a photograph, subject to proof that such processing is unlawful or unauthorized. Such a person would have a challenging time establishing a lawful criteria for the processing of the said information. In the issue brought before the NPC, two alleged acts are involved: the taking of a photograph in a public space of people who did not expect to be photographed, and the subsequent posting with a ridiculing comment. Such acts will not be justified under legitimate interest because they have no apparent justifiable purpose, while exposing and negatively affecting the data subjects. Should the person try and claim that the processing was for an artistic or journalistic purpose, he'd also find that hard to establish given the context of the photograph and its subsequent posting.

Situations like that may be the basis for an action for damages. In the United States, the public disclosure of private facts and publicizing a person in a false light may be the basis of privacy torts. Similar to this is the Philippine's Civil Code provision providing for interference with private life as a basis for claiming for damages (art 26). A person aggrieved by doxing may generally find remedies under civil law for abuse of rights and privacy violations.

"In this digital age, people still deserve the right to be left alone."

A still unexplored remedy for doxing cases are provisions in the DPA on Malicious Disclosure and Unauthorized Disclosure. Both provisions criminalize acts of disclosing personal information of individuals by a personal information controller or personal information processor or their officials, employees or agents. Malicious disclosure refers to the disclosure of unwarranted or false information about a person, where the disclosure was done with malice or bad faith, while any other disclosure without consent of the concerned individual may be considered unauthorized processing.

Both crimes require that the acts be done by a personal information controller or personal information processor. Under the DPA, an individual who processes personal information in connection with the individual's personal, family or household affairs will not be considered as personal information controller. This means that for doxing to be punishable under the DPA, the disclosure of information through online posting, should not be in connection with the person's personal, family or household affairs. Posting in social media is intended to bring to the attention of the public a particular individual. By its nature and purpose, doxing will generally not be considered as being a personal, family or household affair. Where such disclosure was done with malice or bad faith, and involves either false or unwarranted information, the act of doxing may be malicious disclosure. On the other hand, where the disclosure involves any other personal information and done without consent of the data subject, the act may be punished as unauthorized disclosure.

A viral post could be truthful but it is still just a fragment of a bigger and usually more nuanced truth. Sadly, much of today's digital vigilantism are built on such fragments, enabled in no small measure by a social media algorithm that seems to encourage herd mentality. Ironically, the same herd that cries for "fairness" is itself guilty of depriving the same via doxing. Once the damage to the victim has been done—deserved, or otherwise—no amount of public apology belatedly given could reverse such damage. After all, victims of doxing suffer more than just the immediate online threat, intimidation, or humiliation. They can also experience serious, real-world consequences such as loss of employment, the break-up of personal or business relationships, and strained family ties. Some even become victims of in-person harassment and assault.

Can people not freely express their grievances online? Can people not use social media platforms to voice out their opinions against perceived unacceptable behavior? Are people not allowed to let others know about matters that may be a public concern? Indeed, freedom of speech and of expression are cherished freedoms. While people cannot be prohibited from exercising their rights, these freedoms should be exercised with responsibility and due regard for the rights of others. As has often been said, we should think before we click. In the exercise of these freedoms, we should likewise be accountable in case our acts cause undue harm to others. As our Civil Code provides, "[e]very person must, in the exercise of his rights and in the performance of his duties, act with justice, give everyone his due, and observe honesty and good faith." In the end, it is about respect and fairness. In this digital age, people still deserve the right to be left alone.

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) 7753 5584
✉ info@fma.ph
📍 Unit 203 CRM Building III, No.
106 Kamias Road, East Kamias,
Quezon City

Foundation for Media Alternatives