PHILIPPINE ISP VISIBILITY: TECHNOLOGY, LIMITATIONS, AND RECOMMENDATIONS RELATED TO COMBATTING THE ONLINE SEXUAL EXPLOITATION OF CHILDREN

IJM

ABOUT INTERNATIONAL JUSTICE MISSION

International Justice Mission (IJM) is a global organization that protects people in poverty from violence. IJM and our partners are helping local authorities protect more than 400 million people from violence. As the largest anti-slavery organization in the world, IJM partners with local authorities in 21 program offices in 13 countries to combat slavery, violence against women and children, and other forms of abuse against people who are poor. Our model works side-by-side with local authorities and governments to rescue and restore survivors, hold perpetrators accountable in local courts, and strengthen the public justice system so it can better protect people from violence. This model is replicable and has worked to reduce modern day slavery and violence in programs against commercial sexual exploitation of children, among others.

Learn more at IJM.org

AUTHOR:

Caleb Carroll
Internet Crimes Against Children Specialist
International Justice Mission
Philippines - National Investigation and Law Enforcement Development

CO-AUTHOR:

Nancy Abrajano
NILED Intern
International Justice Mission
Philippines - National Investigation and Law Enforcement Development

ENDORSED BY:

Atty. Gideon Cauton
NILED Director
International Justice Mission
Philippines - National Investigation and Law Enforcement Development

Atty. Reynaldo Bicol
Field Office Director
International Justice Mission
Philippines - Manila Field Office

Atty. Noel Eballe
Senior Lead for Policy and Advocacy
International Justice Mission
Philippines - National Investigation and Law Enforcement Development

GRAPHICS DESIGN AND VISUAL SUPPORT:

Meryll Sarco
Lead
International Justice Mission
Philippines – Brand and Communications

Hannah Greer
Communications Intern
International Justice Mission
Philippines – Brand and Communications

This original work is a product of International Justice Mission and was initially published October 2020.

Abstract

Ever since the global technology explosion of the 1990s and 2000s, there has been much confusion about the information that an internet service provider (ISP) can see (versus an electronic service provider (ESP)). The technology that exists today needs a modern, nuanced review in order for government and non-government actors to understand where ISPs fit into solutions to combat the online sexual exploitation of children. The expectation for faster processing of these specialized cases by law enforcement officials and prosecutors is difficult to achieve when existing technology does not match up to the volume and methodology of child sexual exploitation material (CSEM) being released on the web.

Current technologies show improvement; however, sexually motivated offenders can use other formats readily available on the surface level of the internet, such as live streaming, which makes CSEM more challenging to trace and identifying online sexual exploitation of children victims difficult. Recognizing the need for ISPs, and those evaluating their efforts, to re-position and re-conceptualize their role in these cases can substantially affect the success of identifying online sexual exploitation of children cases while simultaneously allowing law enforcement authorities and prosecutors to act more efficiently.

This briefing paper reports in terms of: (1) defining the history of ISPs and their relationship to technology; (2) uncovering the current exchange methods available for sexually motivated offenders to utilize; and (3) providing recommendations gained through analyzing the technology hurdles to blocking CSEM and online sexual exploitation of children. This body of information gathering shows that ISPs' participation and involvement in online sexual exploitation of children cases are important to produce positive results in regard to the outcome of identifying and deterring both financially and sexually motivated offenders and, more importantly, to rescuing the children being sexually abused.

ISPs and ESPs Defined:

Internet Service Provider (ISP) – a company that provides subscribers with access (a connection) to the internet.

Examples: Globe, Smart, Converge, PLDT, etc.

Electronic Service Provider (ESP) – a company or entity that provides technologies, processes, or platforms which allow a user to engage in advertising, selling, messaging, video chatting, etc. via the internet.

Examples: Facebook, Instagram, Snapchat, Skype, Zoom, LinkedIn, Microsoft365, etc.

Keywords: Internet Service Providers, Technology, Online Sexual Exploitation of Children

ISP Visibility and Technology

The question of what an internet service provider (ISP) can and cannot see has been a source of much discussion over the last decade. Most of the conversation's context has been around the concern of users in regard to their privacy online. For a long time, ISPs, Electronic Service Providers (ESPs; such as Facebook, Instagram, etc.), and other secondary apps have sold their users' information for commercial interests. This big business of data analytics recently came to light after the 2016 United States (US) Presidential Election when Cambridge Analytica was found to be buying data and profiling voters via apps and content on the Facebook platform. Since that moment, there has been a more pronounced push from technology companies to make their content and platforms more secure. From the perspective of personal freedoms, liberties, and privacy, this is an excellent thing. It should be clearly stated that this briefing is not an advocacy against privacy rights of users online, recognizing much internet activity is not directly predatory and, in many cases, is based upon good intentions. Indeed, people's devices have become a part of who they are and how they connect and interact with the world. In fact, when handing down a 2014 US Supreme Court decision on a smart phone privacy case, Chief Justice John G. Roberts, Jr. stated that cell phones had become, "Such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[1] While this is clearly a US Supreme Court case, it is important to note that the Republic of the Philippines is similarly concerned about the privacy and rights of its citizens. Additionally, the right to privacy of a person is a fundamental principle in most democratically minded governments in the world. It is interesting to note that this opinion was from nearly six years ago and in that time, smart devices and data privacy has become a more prevalent issue, not less of one.

That said, there is a segment of internet activity that is nefarious in nature. Whether fraud, hacking, cyberattacks or otherwise, technology crime is growing and spreading like wildfire. It is the natural order of how crime, of any type, is realized and progresses. While tech industry experts work to create ways to make people more safe from those criminals, their efforts to protect data unintentionally benefits another section of technology-facilitated crime: the online sexual exploitation of children. Unfortunately, efforts to counter other crime types and increase privacy can create complications for protecting children. This is well known within the law enforcement and advocacy community and is a major concern, especially as Facebook prepares to move their Messenger platform to full end-to-end encryption (E2EE).

Republic Act (RA) 9775, also known as the Anti-Child Pornography Act, Section 9, indicates what an ISP must do to help protect children in the Philippines. The sub-section of focus for this piece, and the subject of much conversation at this time in the Philippines is, "All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered."[2] This begs the question: what exactly can ISPs see in a subscriber's internet activity and what exactly can they do about it? In order to address this, it is helpful to understand the technology involved. Then the issue of whether there is existing technology that would allow an ISP to block content containing child sexual exploitation material (CSEM) effectively can be more fully understood and explored.

What exactly can ISPs see in a subscriber's internet activity and what exactly they can do about it? In order to address this, it is helpful to understand the technology involved. Then the issue of whether there is existing technology that would allow an ISP to block content containing child sexual exploitive material (CSEM) effectively can be more fully understood and explored.

[1] Liptak, A. (2014, June 25). Major Ruling Shields Privacy of Cellphones. Retrieved from https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html

[2] (n.d.). Retrieved from https://lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html

Internet Activity and Existing Technology

To fully explore this issue, an individual needs to look at the technology that exists today. This should be explored through the perspective of both an ISP and an everyday user. It is common knowledge that the internet connects numerous computers together all around the world. This connectivity allows people to instantly find out information, stay abreast of current events, and remain close to loved ones. In order to access it, an ISP provides a connection from the user, and whatever app or device they may be using, to another user. This is often referred to as the ISP providing the "last mile of the road" (Swire et al., 2016). To think of the ISP like a roadway is a powerful analogy. The question to ask is whether the ISPs are just the pavement underneath the tires or are they more like highway patrolmen looking into the vehicles?

1.1 Surfing the Web and HTTPS

It makes perfect sense that a person would assume that since the ISP owns the connection that they can also see everything that is going on when a user is online. In the early days of the internet this may have very well been the case. It is an oversimplification of how it all actually worked, but in historic principle there is much truth behind this idea. Even today, the statement is often proclaimed that ISPs must be watching what we are doing because an individual can search for an item and then their browsers and social media will be filled with ads for that same genre of item. While this is an excellent example of ESPs collecting metadata, this is not typical data that the ISP collects, maintains, and monetizes.

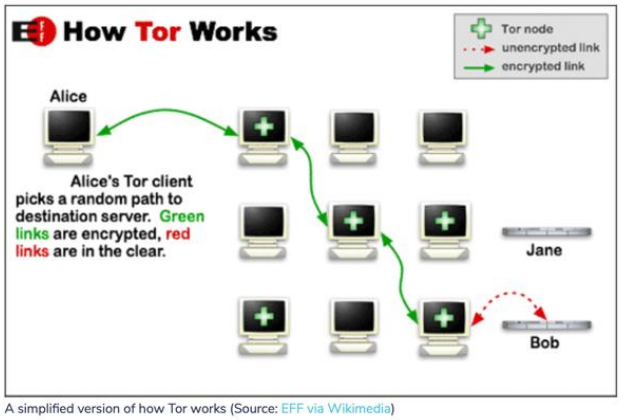
As data privacy became a greater issue, however, things began to change. One of those major changes was the adoption by many sites to begin using a secure and encrypted connection, which is seen in the hypertext transfer protocol secured (HTTPS) format. HTTPS was a change in internet protocol that included more security by forcing authentication of the website, and by maintaining data integrity in preventing leakage from the site itself.[3] This change to websites created a more secure connection and was one of the first steps in the data protection movement. It was a great step forward because now, most banks and websites needing security use this method. However, the HTTPS website encryption still allows ISPs to know a lot of information about their user. For example, it can be seen which uniform resource locator (URL) and domain name system (DNS) were accessed, how long a user was there, when it was accessed, and even the size of the data packets that were sent back and forth. This information is commonly known as "side channel" data mining (*Is your ISP watching you?*, 2018). This, by itself, is still extremely powerful (and lucrative) information. It is relatively easy to see the search queries of a user, how many times they visit a certain website, and to create profiles of websites they are visiting. While the ISP may not be able to see what exactly it is the user is doing on the site, they know the specific site the users are on and have an idea about how much data is moving back and forth.

Unfortunately, while it is helpful for developing advertisements and creating a profile of a user's clear web activity (the clear – or surface - web is the internet which everyone uses and easily displays via search engines), in the context of RA 9775, this isn't helpful. Mainly because, while it does exist limitedly on the clear web, CSEM and child exploitation are not easily locatable in traditional web browsing platforms by people that don't already have an idea where to look. When it does, it is many times pulled down by hosts for child safety reasons. Likely they are also concerned about their servers being seized by the host-home government as well (depending on where the servers are housed). Searching Google and perusing pornography sites around the regular internet is not a typical way that most CSEM is exchanged. That said, it should be clarified that most CSEM exchange and online sexual exploitation of children does not occur under the veil of the dark web either. It largely occurs on surface level ESP platforms that people routinely use every day, such as Skype, Facebook, and many others.

3 Is your ISP watching you? Do ISPs sell your data? (2018, November 7). Retrieved from https://www.le-vpn.com/is-your-isp-watching-you/

The Dark Web and Current Exchange Methods

Then, if CSEM is not exchanged through the regular internet, or clear web, how does it go from user to user? Again, it should be reiterated that most CSEM is exchanged on surface level ESP platforms. More often than not, it is not accessed on actual clear web-level website locations. With that caveat, the following is presented simply to understand alternate ways that sexually motivated offenders access their sexual abuse materials, at times, so that a full knowledge of existing hurdles for ISPs can be appropriately developed and nuanced. And the answer is that it depends on the type of content and the source of it. In many western countries, sexually motivated offenders sometimes use other discreet methods to search for CSEM content. This section is not meant to be an exhaustive evaluation of every possible tool in this realm, but to provide a basic understanding of what exists. One tool that is utilized to access the internet and connect with likeminded individuals is **The Onion Router (Tor).**



A simplified version of how Tor works (Source: EFF via Wikimedia)

Figure 1

Tor was created in the 1990s by the U.S. Navy to give users greater anonymity by securely encrypting their internet traffic.[4] Without getting into too much technical detail, internet activity is encrypted and then passes through a series of relays and, sometimes, bridges. The traffic passes through different computers and, ultimately, the only thing that is visible is the exit relay, which is basically a random computer not associated with the content. Additionally, while some encryption integrity is lost with each exchange, the information is re-encrypted as it passes through each relay. A simplified visual of this is displayed in Figure 1.

This, along with torrents, are what many people know as the dark web today, even though there is much more to it. There are three different troves of "data stores", for lack of better terminology, on the web. The clear net, which was discussed earlier. Then there is the deep net, which is likely public content that simply is not categorized and not searchable. Maybe the information is too old or otherwise, either way search engines like Google would not crawl for it to try and locate it. Then there is the dark web, of which Tor is one part; operating via .onion links. This is content that is only accessible if a user knows the .onion link and has a Tor browser. It is not the regular internet that most people use and there is a substantive amount of illicit activity occurring, hence it is called the dark web. It is important to note that there are legitimate uses for Tor browsing and legitimate sites involved with it. It is especially good for those who are extremely security conscious as the exit relay can typically not be traced back to the user who initiated the traffic. Admittedly, though, much dark web traffic is hidden for nefarious reasons.

4 Annon, D. (2019, July 4). What is the Tor Network and Browser and how can you use it safely? Retrieved from https://privacy.net/what-is-tor/

The second method that sexually motivated offenders use to access and find CSEM around the globe (and particularly in Western countries) are torrents. This is a system of sharing files where the torrent software, often BitTorrent or uTorrent, will search for key words and locate images, videos, and other content, and then allow it to be downloaded for free. For instance, a user would search for whatever they want such as a pirated movie not released publicly yet. That user's torrent software would find multiple other computers sharing the same movie, called seeds, and download pieces of the file from each computer. These computers all interacting with one another are called a swarm and make tracing who the file came from extremely difficult because it came from multiple sources. Figure 2 illustrates how torrents work. There are many legitimate files being hosted by Peer-to-Peer (P2P) protocols utilizing torrents. Again, as a reiteration, a majority of online sexual exploitation of children activity takes place on surface level platforms, however torrents are a known and growing method of CSEM exchange.

The good news is that there are some technologies that have been created to search these torrents and identify CSEM utilizing PhotoDNA and image hashing. Those technologies, and their limitations related to combatting online sexual exploitation of children in the context of the Philippines, will be discussed later. There are a couple of pieces of bad news that go with Tors and torrents though. First, ISPs can block this kind of internet traffic from their service if they know where the relays are or are able to identify torrent traffic being transmitted. That alone is relatively complicated, but doable with a team dedicated to it. However, it is extremely easy to bypass blocks and get around these security measures. Tors have a protocol called Pluggable Transports (PTs) which jumble things around in such a way that the encrypted traffic does not look like Tor traffic anymore. [5] These bridges are not publicly known and are shared amongst Tor groups but are easy to find and gain access to through a simple Google search and some communication. The Tor Project believes that their getting around these blocking measures is a censorship and privacy issue. That is a valid position considering it is not the intended purpose of Tor to create a safe haven for sexually motivated offenders; but that is an unintended major side effect of the system.

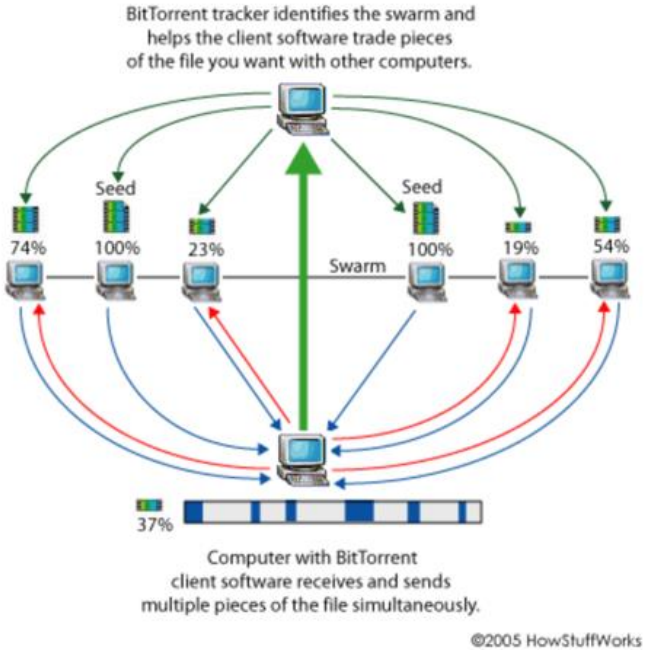


Figure 2

Torrents are just as easy to work around blocking mechanisms, if not easier. One can simply utilize a virtual private network (VPN), which is a legitimate, and common, personal privacy and business mechanism, or engage in their torrenting through Tor connections. While Tors and torrenting are not the primary driving method of CSEM exchange and online sexual exploitation of children in the Philippines currently, they are important for government, tech, and community leaders in the Philippines to understand because they are used generally within the country.

Figure 3 shows Tor directly connected users (not including bridge users or otherwise) over the year 2019,

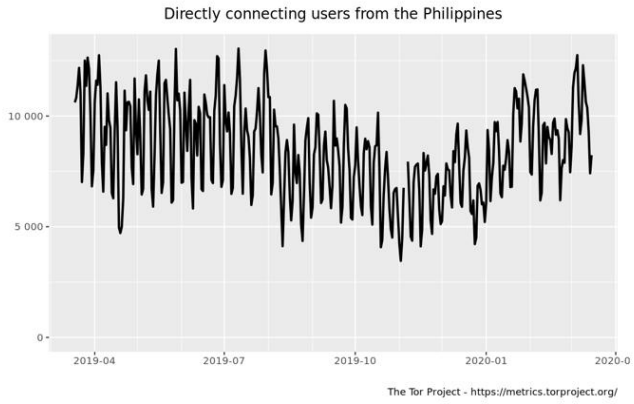


Figure 3

[5] Breaking through censorship barriers, even when Tor is blocked. (2016, August 3). Retrieved from https://blog.torproject.org/breaking-through-censorship-barriers-even-when-tor-blocked

and a Google search of torrenting being blocked in the Philippines yields many discussion boards of successful ways to get around said blocking. And, because this point can't be reiterated enough, based on extensive time engaged with Philippine law enforcement in collaborative casework, International Justice Mission (IJM) simply has not found this to be the way that CSEM is primarily exchanged. Nor is it the major issue fueling online sexual exploitation of children in the Philippines.

In reality, the Philippines has a very real problem of newly created content of child sexual abuse which is custom-ordered by sexually motivated offenders in other places, typically western countries. This can be via pre-planned videos and pictures, but largely occurs via livestreaming where the sexually motivated offender is directing, orchestrating, and viewing the sexual abuse of the child in real time. Most major video chatting platforms, such as Skype, encrypt video calls app-to-app.[6] As such, an ISP would likely be able to see that a video call is occurring based on profiles of the data packets being sent and received, but would not have any idea whether the content is CSEM. Skype notes, as an exception, when the call is directly to a phone number or other means, that it is not encrypted; but that Skype-to-Skype video calls are.

Facebook Messenger is currently in production, testing, and attempted implementation on encryption, and they will most likely encrypt their entire platform for text, call, and video relatively soon (within the next few years).[7] If that takes place, and it is widely believed that, while there are challenges which have to be addressed, sometime in the near future almost all major chatting and video platforms will be E2EE. This means that the data is packaged up by the sending device in a secure manner and is then sent to the receiver's device, which decrypts it. No one in between, without extremely time extensive and invasive means, can see what this data is, other than it is a data packet traveling through the internet. This is a mountain that international law enforcement and the small niche of the tech industry who are dedicated and passionate about child protection are working on but have not entirely figured out how to climb yet. Aside from that, ISPs will not be able to see this content and there currently is no way to detect and block it even if they could.

1.2 VPNS

The other thing that puts the blinders on ISPs are Virtual Private Networks (VPNs). Many times, VPNs get lumped by people outside the technology and internet sectors into the same category as Tors and torrents, but that could not be farther from the truth. Whereas Tor allows a connection which has, arguably, a substantial amount of illicit activity taking place, VPNs are predominantly used for perfectly legitimate reasons. These connections typically allow a user to remotely access a network at a different location than they are currently connecting to the internet. Additionally, the data is encrypted as it is sent, giving VPNs a great deal of security benefit. These are very commonly used with major businesses, governments, and security conscious individuals who do not have any desire or need to delve into the dark web. Certainly, there are people who utilize them for criminal reasons, but the dominant use is for reasonable and legal purposes. Because they are used for so many important things in a positive way, it is not ethical, responsible, or feasible to block them entirely. In the context of this briefing, though, it is important to recognize them as an additional limiter on what user activity ISPs can see.

VPN use in the Philippines is quite high. In fact, the Philippines rates in the top ten for percentage of internet users utilizing a VPN. In the Philippines, twenty-five percent of cybercitizens access a VPN. In contrast, the US and Australia have five and four percent, respectively, of users utilizing a VPN.[8] A major difference to recognize lies in the reason people utilize VPNs. In the US, the majority of users use a VPN to be anonymous online (thirty-seven percent), while in the Asia Pacific region most users are simply using one to access different entertainment options (fifty-five percent; Zagradanin, 2019).

VPNs are an essential part of combatting other forms of technology facilitated and tech-based crime as well; including things like credit card number theft and fraud. Cybercrime is the largest and fastest growing crime

[6] Does Skype use encryption?: Skype Support. (n.d.). Retrieved from https://support.skype.com/en/faq/FA31/does-skype-use-encryption

[7] Schroeder, S. (2019, October 31). Facebook is testing encrypted video and audio calls. Retrieved from https://sea.mashable.com/tech/7197/facebook-is-testing-encrypted-video-and-audio-calls

[8] Zagradanin, I. (2019, March 21). VPN Usage Statistics: Global Trends in the VPN Industry. Retrieved March 18, 2020, from https://www.geosurf.com/blog/vpn-usage-statistics/

category in the world. It is estimated that it will cost the global economy six trillion US dollars in damages during 2021.[9] Utilizing VPNs will be a very important part of the solution in stopping that, as individuals, organizations, and businesses continue to use these networks. The growth of VPN use worldwide has exploded for a myriad of understandable reasons and the Asia Pacific region uses VPNs more than any other region by percentage (Zagradanin, 2019). Again, this is not a bad thing, but it is another major limiting factor which needs to be understood on what ISPs can see. When a user is utilizing a VPN, the ISP can see almost nothing.

CSEM and online sexual exploitation of children Detection Technology

The other piece to this very complicated puzzle is what technologies currently exist to detect CSEM and online sexual exploitation of children. This is an area of innovation that is still, relatively speaking, in its infancy. As tech companies continue to invest in these innovations, more will come available and there will be a greater capability to protect children. The very strong push for total E2EE in most communication platforms will undoubtedly present unique challenges to these innovations. It will be interesting to see how the brilliant minds in tech development work to overcome that in the future. Nevertheless, it is important for government and community leaders to understand these complications so that current policy can be developed and there is a working knowledge of how future developments will be affected by that policy.

1.3 PhotoDNA and Image Hashing

One of the current mainstream ways that CSEM is identified around the globe is via PhotoDNA, also sometimes called image hashing. This is a technology developed by Microsoft which takes known images, breaks them down into pieces, and assigns a unique hash sequence to the image. This is an admitted oversimplification, but it serves the purpose of this document. This sequencing and photo identification are not changed whether the image is resized, or the file name is changed. Therefore, as law enforcement in the U.S., for example, identifies a particular image as CSEM, that image is then flagged with the National Center for Missing and Exploited Children (NCMEC) as part of their Project VIC program (it should be noted that there are other organizations similarly involved in databasing and combatting CSEM who follow a similar process internationally). The image hash is added to a database and then, based on that database, already identified images of CSEM can be picked up again when they are uploaded to a platform that has the PhotoDNA screening capability. This is an incredible tool in locating and catching sexually motivated offenders and, when released by Microsoft, it was a game changer in protecting children online.

The issue with this technology, and what it does not yet address, is catching new, uncategorized material. An additional issue is that, so far, Philippine law enforcement, through no fault of their own, is not connected to this international effort. There are significant efforts being made to change that by Philippine law enforcement. The Philippine National Police (PNP) and National Bureau of Investigation (NBI) will soon have the terminals and secure connection with access to contribute to this effort through the Philippine Internet Crimes Against Children Center (PICACC). The PICACC is an international collaboration to combat online sexual exploitation of children, led by the PNP Women and Children Protection Center (WCPC) and the NBI Anti-Human Trafficking Division (AHTRAD), along with international law enforcement partners in the Australian Federal Police (AFP) and the United Kingdom National Crime Agency (UK NCA), along with international non-governmental organization IJM. Once they are able to access that database, they will be able to upload known hashes and download the existing hash database. However, this is still limited to known imagery and video, not newly produced or livestreamed content.

[9] Ventures, C. (2018, December 13). Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021. Retrieved from https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html

1.4 AI and Further Efforts

The issue, again, with image hashing is that it is searching for, and locating, known images. Therefore, even if an ISP could see the content of messages (which they typically cannot) and they had the known hash set, it still would not help in the context of the most pressing issue in the Philippines. That is because what is being produced is new content of Filipino children being sexually abused. Image hashing would not detect this because it is not a known image entered into the database. There are some promising and exciting technologies in production to try and create Artificial Intelligence (AI) that could identify an online sexual exploitation of children-related conversation and online sexual exploitation of children material, however they are still in the process of full development and implementation. It is highly encouraging that there are protective tools being developed; and the organizations developing them deserve to be commended. But until those advances arrive, humanity still has a solemn obligation to protect children online.

Recommendations for Now

Up to this point, the hurdles based on current technology and infrastructure have been laid out. To be clear, the issue of asking ISPs to effectively and meaningfully block CSEM is not unique to the Philippines. However, it is important to understand that the capability to do such a thing exists only in places where freedoms of civilians are extremely limited and their access to the world is highly restricted. For this reason, the Philippines is on the "right" side of having to wrestle with this issue. Thus, the Philippines must solve the complicated challenge of combatting online sexual exploitation of children without harming important principles of privacy and human rights for people to be secure in their persons, places, effects, and things.

Certainly, the ISPs are not exempt from contributing to fighting this problem. For the most part, around the world, ISPs are effective and responsive partners to lawful investigations into illegal activity. However, they have the resources and expertise to be innovators in the space and should be treated as partners in finding solutions. Their contribution to the fight, and recognition of the problem, must grow.

The hurdles they face are clearly outlined in this paper. It would be ethically and morally wrong to simply sit back and wait on others to create solutions for this problem. Fundamental to humans is our duty to protect our children. There are things in the context of the Philippines which could be nearly immediately implemented and would result in ISPs becoming a huge part of the solution, versus a much more "hands off" approach seemingly being adopted at the current time. These are current practices and infrastructures that are already in practice, in one form or another, around the world today.

1.5 Require ISPs to Maintain Logs of Assigned IP Addresses

In many nations around the world, including the United States, United Kingdom, Australia, Canada, and many others, ISPs maintain records for several months of what Internet Protocol (IP) address is assigned to a particular subscriber account. To explore this further, it is important to have a working knowledge of what an IP address is and how IP addresses are assigned to a user.

When an individual wants to connect to the internet, the ISP provides a road on which to do that. However, computers do not communicate in names and faces like a human does. At the simplest level, computers communicate everything they do in various series of numbers and codes. This is true in how they connect to the internet as well. In order to communicate with other computers on the internet, an IP address is almost universally necessary to facilitate that communication. An IP address is a unique string of numbers, separated by periods, that identifies an individual computer when connected to, and communicating over, the internet. In a vast majority of cases, the most important IP address in online sexual exploitation of children investigations is the one which is assigned by the ISP to the subscriber's primary router. The router then can develop other protocol based off this IP to allow multiple devices to connect to the internet. Absent of a VPN, they will all be based upon the initial address assigned by the ISP.

There are two ways that ISPs do this assigning. The first is a static IP address. This means the ISP assigns one stationary IP to a user's account. Static IP addresses are a minority of internet connections in the world. First, there are vast amounts of internet users and a finite number of IP addresses. If everyone were assigned a static IP address, planet earth would have long ago run

out of IPv4 addresses and would be making a huge dent into IPv6 numbers at this point. It is expensive for ISPs to assign static IP addresses and, therefore, is also expensive for the user. The other, and most common, way IP addresses are assigned is referred to as a dynamic assignment. The limited number of IP addresses the world has are divided up regionally to ISPs and are recycled from user to user. One user may be utilizing an IP address on Monday and a different one on Friday. Different ISPs own different ranges of IP addresses which they can use to keep their subscribers connected to the internet and these are shuffled around amongst these various customers. In many places, ISPs maintain records and data on what subscriber account an IP address is assigned to. Then, based on legal process, an investigative entity can find out what subscriber that IP address was assigned to as long as they know the date and time the illegal activity, they are investigating took place. Most of the time, reporters who are largely electronic service providers do maintain a date and time that a particular IP address logs onto their particular platform. The only information the ISP maintains is subscriber information such as name, address, phone number, billing information and, when and what IP addresses were assigned to a particular account. This means that the information has a very low privacy value because it is not invasive. They are not maintaining records of people's activity online or monitoring what they are doing, simply keeping track of which subscribers they assign an IP address to.

First, as we have established, it is unlikely the ISP can see much of the user's activity to begin with. Second, this would be extremely data intensive and expensive for ISPs to maintain even if did have some probability of success. However, maintaining subscriber IP assignment records is not data storage intensive, relatively inexpensive to implement, not intrusive, and the technology is already widely available around the world. Currently, ISPs in the Philippines largely do not seem to maintain this data. There is some wording in RA 9775 Section 9 which reads, "All internet service providers (ISPs) shall notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person: *Provided*, That no ISP shall be held civilly liable for damages on account of any notice given in good faith in compliance with this section. Furthermore, an ISP shall preserve such evidence for purpose of investigation and prosecution by relevant authorities." This would lead many to believe that the ISP should report and maintain just the kind of IP address information being discussed here. However, because of

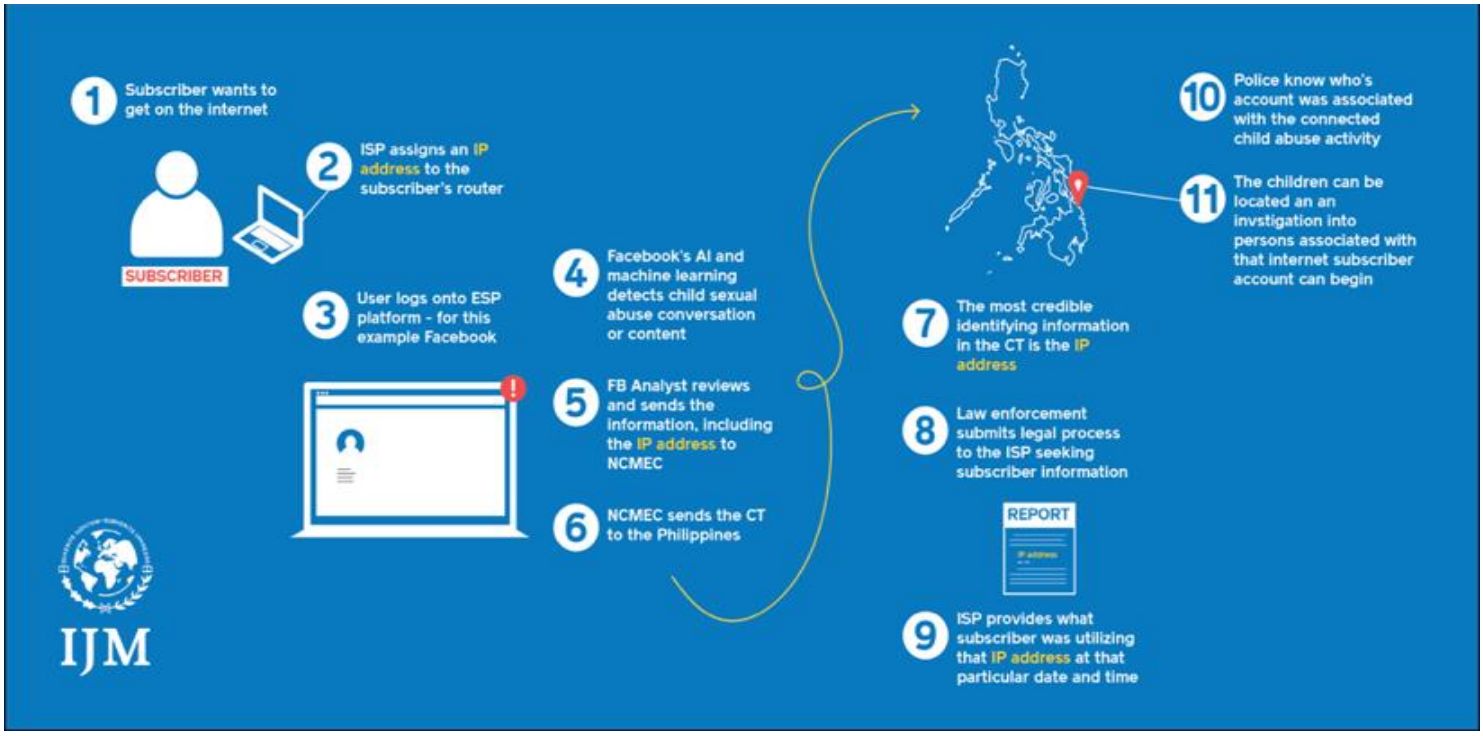


Figure 4

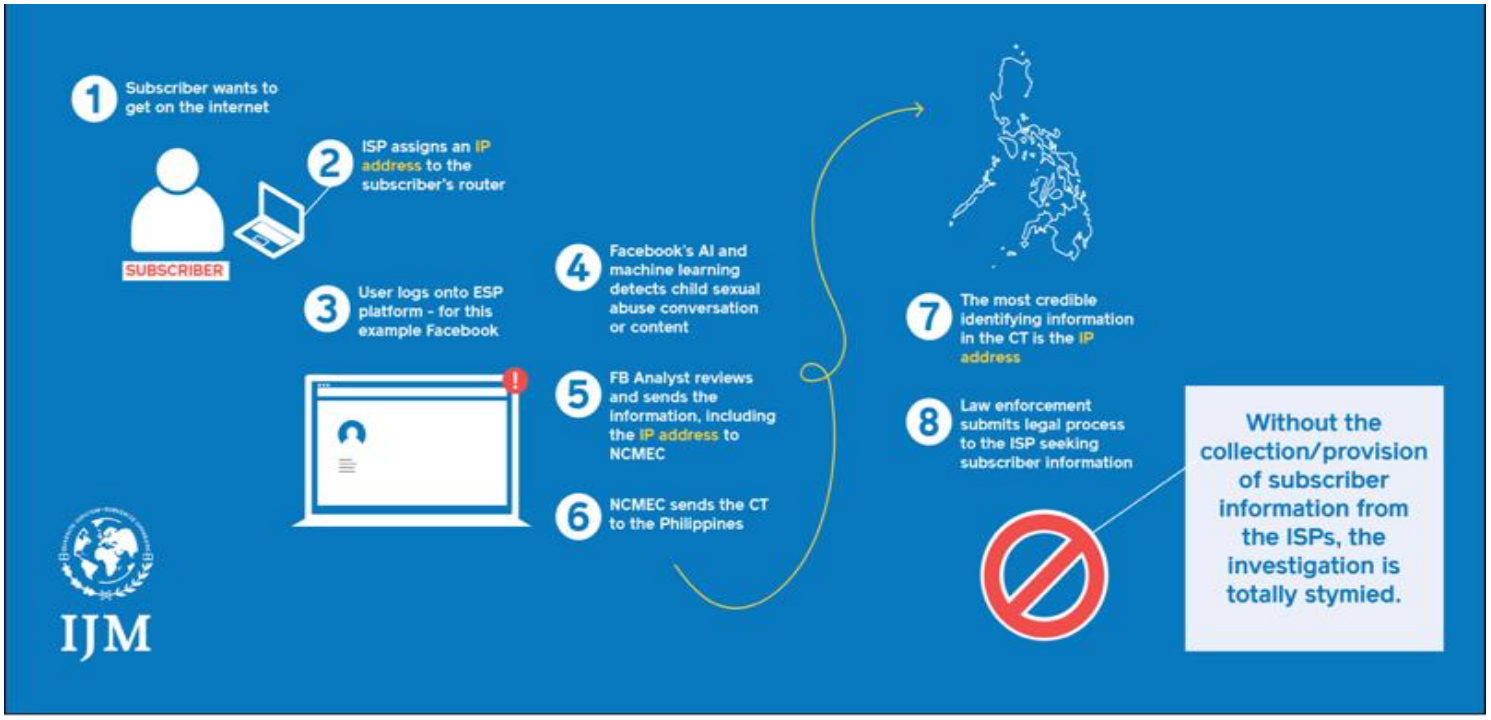


Figure 5

the visibility issues, ISPs normally have no idea that there was CSEM activity until well after the fact; when they are typically notified by an ESP or law enforcement. In this time between the criminal act taking place and the ISP being made aware of it, the important IP assignment information is lost and, often, is unrecoverable. This is no fault of government, law enforcement, or the ISPs. It is simply a gap between written law and real-world application, where important information that could help rescue children is getting lost.

The way that IP addresses are assigned, though, makes collecting IP subscriber assignment information a process that is already consistent with business practices ISPs have in place. ISPs know exactly who they assign an IP address to. This is how they monitor how much data a subscriber has used on their system. They utilize this information to bill people for overages or throttle data speeds if a user has exceeded a certain limit. ISPs in the Philippines would simply need to implement a records management system to maintain this information for a reasonable amount of time. Because these records are simple text-based logs and contain very limited subscriber information, they are not data intensive and would be easy to maintain. This is already a common practice in other nations around the world and is a large way in which ISPs can contribute to combatting online sexual exploitation of children.

This would allow law enforcement officers to more quickly and effectively investigate a case and rescue children being abused. Many ESP reports, such as those from Facebook, give indications a child is being abused but the only definitive, evidentiary information they can provide in their reporting is the IP address used to access the account when the abusive activity was taking place. The ESP provides their recorded subscriber information; however, it is does not have any kind of evidential or substantive value in many instances because users can create fake names, email addresses, and fake other identifying information when they create an account. However, assuming a VPN is not being used, they cannot fake the IP address used to sign in. In the U.S., as just one example, the investigator can then take this IP address and submit legal process to the ISP who tells them what subscriber the IP address was assigned to. The workflow is similar to that displayed in Figure 4. Figure 5 depicts how that process can be stymied if the ISPs do not have, or do not provide, the subscriber information associated with the IP address.

ESPs commonly report suspicious activity surrounding possible child exploitation on their platforms to the NCMEC. This is formatted into a NCMEC CyberTipline Report and sent to the appropriate law enforcement agency. Thousands of CyberTips come into the Philippines every month. In fact, the Philippines Department of Justice Office of Cybercrime (DOJ OOC)

reported during COVID-19 lockdown measures from March 1st, 2020 to May 24th, 2020 that 279,166 CyberTips were sent to them by NCMEC[10]. The important thing to remember is that, in a vast majority of these, IP addresses are the primary identifying element. IP addresses that could potentially be more quickly followed up on to stop the abuse of children.

However, ISPs not maintaining this basic subscriber information and providing it after appropriate legal process means that this very crucial information has absolutely no investigative value. There are potentially thousands of children who cannot be rescued simply because law enforcement has no mechanism to determine who an IP address was assigned to. Requiring ISPs to maintain logs of IP address assignment to their subscribers for a reasonable and specific timeframe would immediately remedy this. It is a low cost, immediate solution that could be applied, which would immensely help in combatting online sexual exploitation of children. Any privacy concerns can be negated by the fact that, again, a person's subscriber information has very low privacy value.

1.6 IPv4 to IPv6 Transition

IP version 4 (IPv4) is the most common protocol used in computer networks compared to the newest application IP version 6 (IPv6). Although the IPv4 version is limited and outdated, IPv6 has emerged to answer those limited capacities in order to become the basic IP. With IPv4 lacking in its development of IP address space, performance-manageability, security, and automatic address assignment (Bouras, Ganos & Karaliotas, 2003),[11] it leaves internet users technologically behind. On the other hand, choosing to transition into IPv6 can ultimately mean less recycling of IP addresses which in turn would make IP logging and identification much easier. Thus, Philippine law enforcement agencies would benefit largely in solidifying a fluid transition into IPv6-only because of its usefulness as a newer IP protocol.

Currently, both the IPv4 and IPv6 are coexisting together through mixed communications, however the IPv6-only application presents itself as a better solution for IP addresses because IPv6-only has the ability to increase the internet's effectiveness by building more security support, eliminating the checksum, (or, a small digital-sized number that is not reliable for verifying data authenticity) from the IP header, being more flexible, efficient renumbering of sites to support multiple addresses on an interface, and supports plug and play operation (Bouras, Gkamas, Primpas & Stamos, 2005).[12] For example, in Figure 6, if all ISPs are operating and supporting IPv6-only hosts, it can make communication easier instead of having IPv4-only hosts and IPv6-only hosts coexisting together.

The heterogenous nature of IPv4 and IPv6 network usage brings more roadblocks to identifying online sexual exploitation of children and a smooth transition of ISPs to employ IPv6 more challenging (Hamarsheh, Goossens, & Al-Qerem, 2012).[13] Removing this roadblock can help law enforcement officials to adequately identify sexually motivated offenders when IP addresses are not recycled as quickly and are logged more effectively. The domino effect is as follows: government legislation can approve IPv4 transition into IPv6, then ISPs can initiate its support towards IPv6 networks allowing for even more effective IP address logging, thus allowing law enforcement agencies to identify and quickly respond to online sexual exploitation of children cases.

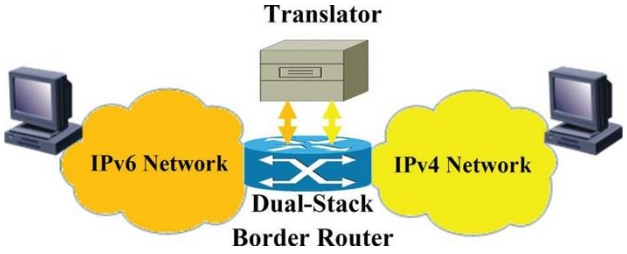


Figure 6

Overall, upgrading to IPv6 gives way for ISPs to have a new technology infrastructure allowing for an easier process to manage IP addresses in a more efficient and

[10] Pulta, B. (2020, May 25). Online child exploitation reports in PH surge amid Covid-19: DOJ. Retrieved July 13, 2020, from https://www.pna.gov.ph/articles/1103852.

11 Bouras, C., Ganos, P. & Karaliotas, A. (2003). The Deployment of IPv6 in an IPv4 world and transition strategies. Retrieved from http://pdfs.semanticscholar.org/b621/6eb9066d925f7cc54fd2d1fe5780d1a02baa.pdf

12 Bouras, C., Gkamas, A., Primpas, D. & Stamos, K. (2005, Apr. 6). Porting and performance aspects from IPv4 to IPv6: The case of OpenH323. Retreived from http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=19090868&S=R&D=a9h&EbscoContent=dGJyMMvl7ESep7E4yOvqOLCmsEiep7dSsqq4S7WWxWXS&ContentCustomer=dGJyMPGqtkqxqrNOuePfgeyx44Dt6fIA

[13] Hamarsheh, A., Goossens, M., Al-Qerem, A. (2012, Mar-Apr.). Assuring Interoperability Between Heterogeneous (IPv4/IPv6) Networks Without using Protocol Translation. Retrieved from http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=83819295&S=R&D=a9h&EbscoContent=dGJyMMvl7ESep7E4yOvqOLCmsEiep7dSs6q4TLWWxWXS&ContentCustomer=dGJyMPGqtkqxqrNOuePfgeyx44Dt6fIA

sustainable manner which is imperative to the long-term growth of the internet. Notably it will also satisfy the request for IP addresses by the growing pool of internet users. The delay in transitioning into IPv6-only will only serve to quicken IPv4's exhaustion. Although IPv6 transition will be costly in the beginning, it is better to adopt IPv6 before IP addresses become exhaustive in the Philippines and other countries. It is also a commitment that was begun around 2011 in the Philippines but has not yet seen realization[14].

With an increase in internet users, a stronger motivation for IPv6 transition is warranted. ISPs and the government have an important role in the transitioning into IPv6 to accommodate the growth of network and internet use, while assisting law enforcement agencies to battle online sexual exploitation of children. The Asia Pacific region "has reached a point of resource crisis and IPv6 readiness is a hard requirement for growing government and private networks" (Levin & Schmidt, 2014).[15] Failure to transition means reducing the capacity of a society to communicate through the global internet. This calls for immediate attention to re-assess the IPv6 transition deployment in the Philippines.

1.7 CSEM URL Lists

One of the requirements of the existing Philippines law surrounding this issue is, as mentioned earlier, RA 9775 and its command to have ISPs "block and filter" CSEM should not be ignored; and it would be remiss not to address it. It has been outlined throughout this briefing why "blocking and filtering" is not currently the panacea that many may feel it is, based on existing technology. Advocacy around these issues should be increasingly careful to understand this so as not to paint ISPs as the proverbial "big bad wolf" unfairly. This is not to say that one day blocking at the ISP level will not be a stronger solution, as technological innovation continues to astound. It simply addresses where "blocking and filtering" stands in the present day.

However, the technological challenges of today, presented by the way this dynamic puzzle fits together, should not absolve ISPs from their responsibility to block what they can. The reality is that, in today's terms, the most ISPs can hope to block with any kind of confidence via their connections are URLs known to be communities of people exchanging CSEM (or information about it) and actual CSEM URL distribution points themselves. ISPs should still be expected to do this as their legally mandated obligation. They are already doing this in a limited way in the Philippines, but the process is cumbersome, not all encompassing, and puts the burden of identifying and notifying the ISPs about these URLs on Philippine government and law enforcement, which are already carrying very heavy workloads, instead of an investment and effort on the part of the ISPs.

There are numerous companies that exist which sell platforms and infrastructure related to this objective. They are often times incredibly expensive. As mentioned, in the Philippines, an infrastructure already exists to block the URLs via current measures implemented by the Philippine National Telecommunications Commission (NTC) and Philippine ISPs. In conjunction with the ISPs, they are able to provide sites that should be blocked, and they are then stopped from Philippine internet traffic (again, absent a VPN or some other means). The issue is that ISPs currently require DOJ OOC, PNP, NBI, and NTC to maintain the list, which is time-exhaustive and, ultimately, burdening down already extremely busy government agencies. This shouldering of the manual effort and maintenance needs to be shouldered by the ISPs as a part of their requirements under RA 9775, and as a component of their corporate social responsibility. The solution does not have to be a for-profit private company providing this technology solution and infrastructure either. The infrastructure, again, largely exists. The only question is where the ISPs could obtain such a regularly updated and maintained list to apply to their existing blocking platforms.

One such solution is the United Kingdom-based Internet Watch Foundation (IWF). They maintain a well-managed, comprehensive CSEM-related URL list and image hash sets that are updated twice daily. This intensive and consistent updating is pushed out to their member organizations and averages more than several

[14] http://region4a.dost.gov.ph/12-updates/532-ph-joins-world-to-change-standard-internet-protocol-from-ipv4-to-ipv6

[15] Levin, S. & Schmidt, S. (2014, Sept. 10). IPv4 to IPv6: Challenges, solutions, and lessons. Retrieved from https://reader.elsevier.com/reader/sd/pii/S0308596114001128?token=0DF34A21262D51CA7A27BF8F5B227800E89FB0C75ED971F66940CC0CD845BBBD238433FE2769D3D1E8FD1FB72A8BE72F

hundred new sites per day being added to the "bad URL" list.[16] This list can be placed into existing infrastructure by the ISPs. Membership does entail a cost which is based upon organizational factors. However, this cost is much less than employing a private company to implement a for-profit solution which, likely, will be developing its list from IWF or other partner organizations. As a credible non-profit organization, IWF is a leader in partnering with industry in this area and is excited to work with ISPs, some of whom they already have membership agreements with. IWF also maintains a highly comprehensive database of image hashes of known CSEM as well. While we have explored the limitations of this in the context of the Philippines (remember that the Philippines has high volumes of new, unidentified, and live streaming content) and with Philippine ISPs (again, they simply cannot see into much of the activity online because of the way it is packaged and exchanged by ESPs), this CSEM hash database could still be limitedly useful now and there will hopefully be solutions in the future involving image hashing which are more applicable to ISPs. Regardless, IWF has that dataset, and membership would allow ISPs access to it for resourcing.

To be clear, this is not to say that for-profit companies in this space are not good or do not have a place. They definitively are doing good work and have a significant part to play in combatting CSEM and protecting children online. This simply would not likely be the most cost-effective solution in the Philippines based on existing technology and infrastructure. This existing infrastructure could be aligned with a non-profit, such as IWF, to achieve the same coverage as a for-profit solution.

Again, at this point in time, blocking these URLs is really the top end of what can actually be fully blocked by an ISP. They simply do not have visibility into the content that is transmitted via the platforms hosted by the ESPs. They truly are the "last mile of the road" in the connection to the internet. This could very well change in the future; but that, again, is for future consideration and there are children being abused now. This solution, along with the other two, would change the dynamic on how online sexual exploitation of children is investigated and countered in the Philippines, bringing immediate relief to countless children.

[16] URL List. (n.d.). Retrieved August 10, 2020, from https://www.iwf.org.uk/become-a-member/services-for-members/url-list

Summary of Recommendations

Emerging technology will be the tools of the future and gives us great hope. However, the Philippines, amongst the rest of the world, cannot sit back and wait for that future technology to happen. There are things that could be actioned now that will result in greater accountability for criminals sexually exploiting children online and would result in children being rescued sooner from the sexual abuse being perpetrated using these technology forums and platforms.

These action items should be worked on immediately and can accomplish these goals:

- Having ISPs maintain logs, for a reasonable and specific time, of the subscriber they assign an IP address to at a given date and time.
- Complete the IPv4 to IPv6 transition to reduce the volume of times a particular IP address must be recycled.
- ISPs obtaining memberships in organizations that can provide regularly updated CSEM-linked URL lists to block those particular sites (such as IWF).

Conclusion

The online sexual exploitation of children is a horrific crime type that merits the world's attention. ISPs have a corporate ethical responsibility to do their part and keep children in their communities safe. That said, based on the world's internet traffic today and the current detection and blocking technologies available to them, ISPs are not positioned well to see the content that is going through their service, nor are they able to detect new content. Even if they could see what was going on, to hire people to manually watch all of the internet traffic for new material would be both an invasion of privacy and a colossal expense. The Georgia Institute of Technology (Georgia Tech; GT) has a working paper that does an excellent job explaining and analyzing the problem[17]. Georgia Tech is a U.S. leader in academia within the tech industry and in cybersecurity. In this document, Swire et al. (2016) deduces that, "ISPs do not have comprehensive or unique visibility into users' online activity." Smart Communications, Philippines Long Distance Telephone, and Globe all admit this is the limit of their visibility in their various privacy policies, listed publicly (see Addendums A, B and C).

An illustration of Swire's conceptualization, from the of this is pictured in Figure 7, which is from their working paper. To put it into words, ISPs can be likened to a water hose. When the source of the water is turned on, it is known that water goes in one side. It can be heard inside the hose and the hose becomes more tense. Out the other end of the hose comes the water. If a person stares at the hose, they cannot see the water inside or what is happening along its journey. In order to actually feel the water, one has to be at either end of the hose. ISPs are the hose and the reality is that they typically cannot see what is going on inside. That has to be detected and seen at both ends (normally ESPs). This requires advances in device technology, continued vigilance in communities, and tireless efforts by international law enforcement. Eventually, there will be some other technology that helps along the way, but until then, the fight must be waged with what is in front of us until all are free.

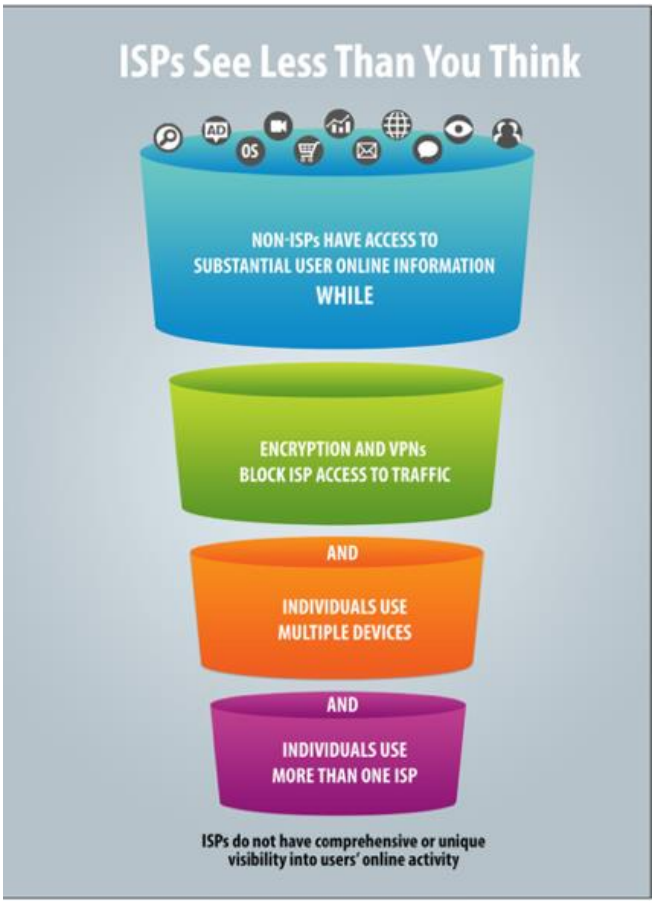


Figure 7

[17] Swire, P., Hemmings, J., and Kirland, A, "Online Privacy and ISPs", May 2016; https://iisp.gatech.edu/working-paper-online-privacy-and-isps

Addendum A

1.8 A.1. Privacy Policy – Smart

PRIVACY STATEMENT[18]

1. Our Privacy Commitment

Smart Communications, Inc. ("SMART") respects our customers' fundamental right to privacy, and we commit to take great care in safeguarding your personal data. SMART has developed a privacy statement that aims to ensure that we adopt and observe appropriate standards for personal data protection in compliance with applicable privacy laws and regulations.

While this privacy statement sets out the general principles that govern the collection, use, and disclosure of our customers' personal data, we have also developed this privacy statement to inform you more specifically about our privacy practices.

2. Why we collect your personal data

Throughout your use of our services, we collect and maintain some basic information about you. We do so only for the purposes and legal bases described below.

1. We process your personal data to perform our obligations under contract with you.
    - **To create and nurture a relationship with you,** so that we can continuously provide you with our services. For example, when you apply for any of our services, we collect personal data about you, that will allow us to validate your identity and credit history for purposes of billing and collection of fees for the products and services that you avail from us.
2. We process your personal data based on our legitimate interest to function effectively as a business, but we only do so when your interests and fundamental rights or freedoms do not override our legitimate interest.
    - **To continuously improve our business and operations.** For example, we analyze your usage of our network and facilities to help us manage your account, provide customer care activities, investigate and resolve your service-related requests and concerns, monitor the quality and security of the network, train our staff, and plan for future growth. We may also process your personal contact details and publish them in an internal directory listing, in order to effectively communicate with you and provide you with necessary assistance.
    - **To continuously improve our products and services.** We collect, use, process, and analyze your use of our products and services so that we can understand how to improve them for your benefit. Our analysis may include some information about your usage, such as the volume and frequWe process your personal data as you avail of our products and services so that we may be able to create and offer better products and services for you, including through direct marketing. We only carry out these processing activities based on your consent.ency of your use of our SMS, voice, and data services, and your historical locational information which we determine based on an analysis of the places where you may have used our products and services in order to generate insights on foot traffic, crowd density, and mobility patterns.
    - **To understand your needs and preferences so that we can serve you better.** We process data to determine your usage profile by maintaining a record of the products and services that you avail from us, and by analyzing other activities such as when you participate in our market research initiatives, when you visit and transact in our stores, and when you visit and use our websites and mobile apps. We do so in order to gain a better insight about the kinds of offers that would be relevant to your preferences.

[18] https://smart.com.ph/Corporate/privacy

- **To manage the security of our business operations.** We may process your personal data to conduct IT security operations, to manage our assets, to ensure your fair use of our products and services, and for business continuity, disaster recovery, and audit purposes.

3. We process your personal data as you avail of our products and services so that we may be able to create and offer better products and services for you, including through direct marketing. We only carry out these processing activities based on your consent.
    - **To send you offers, recommendations and promotions.** We process your usage profile to send you customized offers and promotions through your contact details using channels such as SMS, voice calls, and e-mail. This includes location-based offers that are exclusively available in areas that you may frequent.
    - **To elaborate your usage profile.** We may also collect personal information about you from third-party sources such as our subsidiaries, affiliates, and business partners, to whom you have also given your consent for them to share your information with us. We create this enhanced usage profile about you solely to get a deeper understanding of your preferences so that we can send you even better targeted product recommendations, special offers, and promotions
4. We process your personal data to comply with legal requirements.
    - **To assist public authorities.** We generate statistical insights based on your usage of our network and facilities to assist public authorities in planning for healthcare, disaster management, and other similar initiatives. When we can, we aggregate and anonymize this information so that you are never identified as an individual.
    - **To comply with legal requirements.** We run credit scoring programs and initiatives, including but not limited to, providing information to the Credit Information Corporation in accordance to Republic Act No. 9501 and the Credit Information System Act. We may also perform other required personal data processing or disclosure to meet other relevant legal and regulatory requirements.

3. How we collect your personal data

We collect your personal data from several resources.

Information you share with us
Most of the personal data we retain are information you have shared with us. You provide us with personal data when you:

- Apply for our services by filling out application forms, subscription agreements, and other similar or related documents through any of our available channels (online, in our stores, or through our sales representatives);
- Get in touch with us to ask about something, file a complaint or request for service;
- Take part in our research and surveys; and/or

Information we collect during our relationship with you
We also collect information as you use our products and services, like when you:

- Use our network, facilities and services - whether it is Mobile, Fixed, Home, or any of our other products, services, and channels;
- Pay your bills or purchase add-on products and services;
- Use our apps, websites, and self-service channels and portals;
- Join our promos, prize raffles, or rewards & loyalty programs;
- Participate in our market research activities; and
- Visit and transact in our stores.

Information we collect from other **sources**
We may also collect your personal data, from our subsidiaries, affiliates, and business partners, to whom you have also given your consent for them to share your information with us.

For a list of these partners, please visit https://smart.com.ph/Corporate/privacy#affiliates.

4. When we disclose your personal data

There are a variety of circumstances where we may need to share some of the information that you have provided to us. In these cases, we ensure that your personal data is disclosed on a confidential basis, through secure channels, and only in compliance with applicable privacy laws and regulations.

We will never share, rent, or sell your personal data to third parties outside of SMART except in special circumstances where you may have given your consent for, and as described in this statement.
In some instances, we may be required to disclose your personal data to our agents, subsidiaries, affiliates, business partners and other third-party agencies and service providers as part of our regular business operations and for the provision of our products and services. This means we might share your information with:

- **Our service providers, contractors, and professional advisers who help us provide our products and services.** This includes partner companies, organizations, or agencies, and their sub-contractors. For example: our couriers for bill delivery and our customer contact centers for our pre- and post-sales hotline operations;
- **Our subsidiaries and affiliates with whom you have also signed-up with.** We do so only for the improvement of each other's legitimate business and operations. For example: we share information with each other about your usage profile so that we can create new offers that bundle our products and services into a single subscription;
- **Other companies to whom you have also given consent for us to share your information with.** For example, when you sign-up for products and services offered by other companies, they may request for information from us in order for them to validate your identity; and
- **Law enforcement and government agencies,** but only when required by laws and regulations and other lawful orders and processes.

For the list of our partners, please visit: https://smart.com.ph/Corporate/privacy#affiliates.

5. How we protect your personal data

The integrity, confidentiality, and security of your information are important to us. That's why we strictly enforce our privacy statement within SMART and have implemented technical, organizational, and physical security measures that are designed to protect your information from unauthorized or fraudulent access, alteration, disclosure, misuse, and other unlawful activities. These are also designed to protect your information from other natural and human dangers.

We also put in effect the following safeguards:

- We keep and protect your information using a secured server behind a firewall, encryption and security controls;
- We keep your information only for as long as necessary for us to (a) provide the products and services that you avail from us, (b) for our legitimate business purposes, (c) to comply with pertinent laws, and (d) for special cases that will require the exercise or defense of legal claims and for a maximum retention period of twelve (12) years from your service's permanent deactivation.
- We restrict access to your information only to qualified and authorized personnel who are trained to handle your information with strict confidentiality;
- We undergo regular audits and rigorous testing of our infrastructure's security protocols to ensure your data is always protected;
- We promptly notify you and the competent data protection authority, when sensitive personal data that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person;
- We let you update your information securely to keep our records accurate.

6. What your choices are

You are afforded certain rights in relation to your personal data under applicable data privacy laws and regulations.

You are entitled (in the circumstances and under the conditions, and subject to the exceptions, set out in applicable law) to:

- **Request access to the personal data we process about you:** this right entitles you to know whether we hold personal data about you and, if we do, to obtain information on and a copy of that personal data.
- **Request a rectification of your personal data:** this right entitles you to have your personal data corrected if it is found to be outdated, inaccurate, or incomplete.
- **Request the erasure of your personal data:** this right entitles you to request the erasure of your personal data, such as in cases where your personal data is no longer necessary to achieve the legitimate business purpose of its use or processing.
- **Request the restriction of the processing of your personal data:** this right entitles you to request that we only process your personal data in limited circumstances, including with your consent.
- **Request portability of your personal data:** this right entitles you to receive a copy of personal data that you have provided to us (in a structured, commonly used and machinereadable format). This includes requests for us to transmit a copy of such personal data to another company, on your behalf.

You moreover have a right to object to the processing of your personal data, such as in cases when we process your personal data for purposes related to direct marketing.

To the extent that the processing of your personal data is based on your consent, you have the right to withdraw such consent at any time by contacting our Data Privacy Officer. Please note that this will not affect the lawfulness of the processing that was carried out before you withdrew your consent or SMART's right to continue parts of the processing based on other legal bases than your consent. If, however we have not provided you with another legal basis justifying the processing of your personal data in this privacy statement, we will stop the processing and delete your personal data. To exercise these rights, you may get in touch with our Data Privacy Officer through the contact details provided below. In some instances, we may request for supporting documents or proof before we effect any requested changes to your personal data.

If, despite our commitment and efforts to protect your personal data, you believe that your data privacy rights have been violated, we encourage and welcome individuals to come to SMART first to seek resolution of any complaint. You have the right at all times to register a complaint directly with the relevant supervisory authority or to make a claim against us with a competent court (either in the country where you live, the country where you work or the country where you deem that data privacy law has been infringed).

SMART Data Privacy Office
6799 Ayala Ave., Makati City, 1226, Philippines
Email: dataprivacyoffice@smart.com.ph

7. Changes to our privacy statement

From time to time, we may update our privacy statement and practices to comply with changes in applicable laws, to comply with government and regulatory requirements, to adapt to new technologies and protocols, to align with industry best practices, and for business purposes.

You will always be provided notice if these changes are significant and, if we are required by law, we will ensure to obtain your updated consent.

This Privacy Statement is effective January 15, 2020.

Website Privacy Policy

The policies below are applicable to the Web site and affiliate sites of Smart Communications, Inc. (SMART) found at www.smart.com.ph . Please be advised that the practices described in this Privacy Policy apply only to information gathered online at our Web site. They do not apply to information that you may submit to us offline or to Web sites maintained by other companies or organizations to which we may link or may have link through us.
By visiting our Web site, you are accepting the practices described in our Privacy Policy. If you do not agree to the terms of this Privacy Policy, please do not use the Web site.

SMART collects personal information, voluntarily submitted by visitors to the Web site, which enables us to respond to requests for publications, distribute e-newsletters, process employment inquiries and respond to requests for more information or assistance. SMART adheres to the highest standards of ethical practices in all of our operations and is dedicated to protecting the privacy of all visitors to our Web site. Except as disclosed below, we do not sell, barter, give away, rent or permit anyone outside of SMART to use your personal information.

We occasionally use third-party agents, subsidiaries, affiliates and partners to perform functions such as creative design, marketing, analytics, programming, site maintenance, providing customer service, etc., on our behalf. These entities have access to the personal information needed to perform their functions and are contractually obligated to maintain the confidentiality and security of any personal information collected from the Web site. They are restricted from using, selling, distributing or altering these data in any way other than to provide the requested services to the Web site.
We may also use or disclose your personal information if required to do so by law or in the good-faith belief that such action is necessary to

(a) conform to applicable law or comply with legal process served on us or the Website;
(b) protect and defend our rights or property, the Web site or our users, and
(c) act under emergency circumstances to protect our safety and security and those of our affiliates, agents and the users of the Web site or the public in general.

SMART also collects anonymous information to help us tailor the Web site to visitor interests and concerns. We use "cookies" to help us understand which parts of our Web site are the most popular, where our visitors are going and how much time they spend there. The information that is gathered through cookies is used solely to assist in improving Web site design and function. This Web site is functional without the retention of cookies. You may elect to block cookies from this site through your browser settings. SMART strives to protect the transmission of any information submitted by visitors. SMART does not warrant that transmission of data will be completely secured, and any and all submissions are at the visitor's risk.

This Web site may contain links to sites operated by third parties. Please be advised that the practices described in this Privacy Policy do not apply to information gathered through these other Web sites.

Please remember that any information that you may share in public areas, such as message boards or feedback sections, becomes public, and therefore this Privacy Policy does not apply to any information you choose to make public. Please be careful about what you disclose, and do not post any personal information that you expect to keep private.

The Web site is published in the Republic of the Philippines and is subject to laws of the Republic of the Philippines. If you are located in a country outside the Republic of the Philippines and voluntarily submit personal information to us, you thereby consent to the general use of such information as provided in this Privacy Policy and to the transfer of that information to, and/or storage of that information in, the Republic of the Philippines. SMART shall not be liable under any circumstances for damages resulting from use of information collected from visitors to the site.

SMART may change this Privacy Policy to reflect, among others, changes in the way we collect visitor information. Questions and comments should be directed to this email address.
Last updated: January 21, 2009

Addendum B

1.12 A.2. PLDT Group Data

PLDT Home Data Privacy Notice[19]

We respect your fundamental right to privacy and we commit to take great care in safeguarding your personal data. Throughout your use of our services, we collect and maintain some basic information about you. In accordance with applicable privacy laws, we share with you the general principles that govern how we collect, use, and share your personal data, as well as our privacy practices.

Why we collect your personal data
When we process your personal data, we do so under the following legal bases and for the purposes set out below:

1. We process your personal data to perform our obligations under contract with you.
   - **To create and nurture a relationship with you** so that we can continuously provide you with our services. For example, when you apply for any of our services, we collect personal data about you, that will allow us to validate your identity and credit history for purposes of billing and collection of fees for the products and services that you avail from us.
2. We process your personal data based on our legitimate interest to function effectively as a business, but we only do so when your interests and fundamental rights or freedoms do not override our legitimate interest.
   - **To continuously improve our business and operations.** For example, we analyze your usage of our network and facilities to help us manage your account, provide customer care activities, investigate and resolve your service- related requests and concerns, monitor the quality and security of the network, train our staff, and plan for future growth. We may also process your personal contact details and publish them in an internal directory listing, in order to effectively communicate with you and provide you with necessary assistance.
   - **To continuously improve our products and services.** We collect, use, process, and analyze your use of our products and services so that we can understand how to improve them for your benefit. Our analysis may include some information about your usage, such as the volume and frequency of your use of our voice, and data services, and your historical locational information which we determine based on an analysis of the places where you may have used our products and services in order to generate insights on foot traffic, crowd density, and mobility patterns.
   - **To understand your needs and preferences so that we can serve you better.** We process data to determine your usage profile by maintaining a record of the products and services that you avail from us, and by analyzing other activities such as when you participate in our market research initiatives, when you visit and transact in our stores, and when you visit and use our websites and mobile apps such as MyPLDT Smart App. We do so in order to gain a better insight about the kinds of offers that would be relevant to your preferences.
   - **To manage the security of our business operations.** We may process your personal data to conduct IT security operations, to manage our assets, to ensure your fair use of our products and services, and for business continuity, disaster recovery, and audit purposes.
3. We process your personal data as you avail of our products and services so that we may be able to create and offer better products and services for you, including through direct marketing. We only carry out these processing activities based on your consent.

[19] https://pldthome.com/privacypolicy

- **To send you offers, recommendations and promotions.** We process your usage profile to send you customized offers and promotions through your contact details using channels such as SMS, voice calls, and e-mail. This includes location-based offers that are exclusively available in areas that you may frequent.
- **To conduct online marketing.** We process information such as your mobile number, e-mail address, and browsing behavior, which we collect through cookies and tags (when you visit our websites) in order to place advertisements about our latest products and promotions on some of the most popular social media platforms and websites that you may visit. Please see our cookies policy https://pldthome.com/cookie-policy (https://pldthome.com/cookie-policy) for more details.
- **To elaborate your usage profile.** We may also collect personal information about you from third-party sources such as our subsidiaries, affiliates, and business partners, to whom you have also given your consent for them to share your information with us. We create this enhanced usage profile about you solely to get a deeper understanding of your preferences so that we can send you even better targeted product recommendations, special offers, and promotions.

4. We process your personal data to comply with legal requirements.

- **To assist public authorities.** We generate statistical insights based on your usage of our network and facilities to assist public authorities in planning for healthcare, disaster management, and other similar initiatives. When we can, we aggregate and anonymize this information so that you are never identified as an individual.
- **To comply with legal requirements.** We run credit scoring programs and initiatives, including but not limited to, providing information to the Credit Information Corporation in accordance to Republic Act No. 9501 and the Credit Information System Act. We may also perform other required personal data processing or disclosure to meet other relevant legal and regulatory requirements.

When we disclose your personal data

In some instances, we may be required to disclose your personal data to our agents, subsidiaries, affiliates, business partners and other third-party agencies and service providers as part of our regular business operations and for the provision of our products and services.
This means we might share your information with:

- **Our service providers, contractors, and professional advisers who help us provide our products and services.** This includes partner companies, organizations, or agencies, and their sub-contractors. For example, our couriers for bill delivery and our customer contact centers for our pre- and post-sales hotline operations;
- **Our subsidiaries and affiliates with whom you have also signed-up with.** We do so only for the improvement of each other's legitimate business and operations. For example, we share information with each other about your usage profile so that we can create new offers that bundle our products and services into a single subscription;
- **Other companies to whom you have also given consent for us to share your information with.** For example, when you sign-up for products and services offered by other companies, they may request for information from us in order for them to validate your identity; and
- **Law enforcement and government agencies,** but only when required by laws and regulations and other lawful orders and processes.

In these cases, we ensure that your personal data is disclosed on a confidential basis, through secure channels, and only in compliance with applicable privacy laws and regulations. We will never share, rent, or sell your personal data to third parties outside of PLDT, except in special circumstances where you may have given your consent for, and as described in this statement.

For a list of our partners, please visit https://pldthome.com/privacy-policy-partners. (https://pldthome.com/privacy-policy-partners)

How we protect your personal data

The integrity, confidentiality, and security of your personal data are important to us. That's why we strictly enforce our privacy statement within PLDT and have implemented technical, organizational, and physical security measures that are

designed to protect your information from unauthorized or fraudulent access, alteration, disclosure, misuse, and other unlawful activities. These are also designed to protect your information from other natural and human dangers.

We also put in effect the following safeguards:

- We keep and protect your information using a secured server behind a firewall, encryption and security controls;
- We keep your information only for as long as necessary for us to (a) provide the products and services that you avail from us, (b) for our legitimate business purposes, (c) to comply with applicable laws, and (d) for special cases that will require the exercise or defense of legal claims, and for a maximum retention period of 12 years after termination;
- We restrict access to your information only to qualified and authorized personnel who are trained to handle your information with strict confidentiality;
- We undergo regular audits and rigorous testing of our infrastructure's security protocols to ensure your information is always protected;
- We promptly notify you and the National Privacy Commission, when sensitive personal data that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person; and
- We let you update your information securely to keep our records accurate.

What your choices are
You are afforded certain rights in relation to your personal data under the Data Privacy Act of 2012 (Republic Act No. 10173). You are entitled (in the circumstances and under the conditions, and subject to the exceptions, set out in applicable law) to:

- **Request access to the personal data we process about you:** this right entitles you to know whether we hold personal data about you and, if we do, to obtain information on and a copy of that personal data.
- **Request a rectification of your personal data:** this right entitles you to have your personal data corrected if it is found to be outdated, inaccurate, or incomplete.
- **Request the erasure of your personal data:** this right entitles you to request the erasure of your personal data, such as in cases where your personal data is no longer necessary to achieve the legitimate business purpose of its use or processing.
- **Request the restriction of the processing of your personal data:** this right entitles you to request that we only process your personal data in limited circumstances, including with your consent.
- **Request portability of your personal data:** this right entitles you to receive a copy of personal data that you have provided to us (in a structured, commonly used and machine-readable format). This includes requests for us to transmit a copy of such personal data to another company, on your behalf.

You moreover have a right to object to the processing of your personal data, such as in cases when we process your personal data for purposes related to direct marketing.

To the extent that the processing of your personal data is based on your consent, you have the right to withdraw such consent at any time by contacting our Data Privacy Officer through the contact details provided below, or by accessing https://my.pldthome.com (https://my.pldthome.com). Please note that this will not affect the lawfulness of the processing that was carried out before you withdrew your consent or PLDT's right to continue parts of the processing based on other legal bases than your consent. If, however, we have not provided you with another legal basis justifying the processing of your personal data in this privacy statement, we will stop the processing and delete your personal data.
To exercise any of these rights, you may get in touch with our Data Privacy Officer through the contact details provided below. In some instances, we may request for supporting documents or proof before we effect any requested changes to your personal data.

If, despite our commitment and efforts to protect your personal data, you believe that your data privacy rights have been violated, we encourage and welcome individuals to come to PLDT first to seek resolution of any complaint. You have the right at all times to register a complaint directly with the National Privacy Commission or to make a claim against us with

a competent court (either in the country where you live, the country where you work or the country where you deem that data privacy law has been infringed).

PLDT Group Data Privacy Office Ramon Cojuangco Building, Makati Avenue, Makati City 1200 Philippines dpo@pldt.com.ph (mailto:dpo@pldt.com.ph)

PLDT Home Data Privacy Office Ramon Cojuangco Building, Makati Avenue, Makati City 1200 Philippines homedpo@pldt.com.ph (mailto:homedpo@pldt.com.ph)

You may view our Privacy Policy here (https://pldthome.com/privacypolicy)

Addendum C

1.15 A.3. Privacy Policy - GlobeNoticeTransition

1. Privacy Policy[20]

To create a wonderful world for our customers, partners, community, and the nation as a whole, Globe Telecom, Inc. and its subsidiaries (collectively "Globe," "we," "us," "our") put you, our customers, first. Because we care for you, we regard your privacy with the utmost importance.

This Privacy Policy outlines our policy in relation to the collection, use, and protection of your Customer Data to provide you with a wonderful customer experience. From time to time, we may update our Privacy Policy to reflect current changes in our policy and the law. When we do so, we will notify you by posting it on our website for your information and reference.

2. Your Rights As Our Customer

Globe recognizes that you should be the ultimate decision-maker on matters that involve your Personal Information. To this end, Globe is mindful of the fundamental right to privacy of every Globe customer under the Data Privacy Act of 2012.

By accepting the Terms and Conditions for the use of Globe products and services, you agree to the collection, processing, use, and sharing of your Personal Information in accordance with this Privacy Policy that will enable us to provide you with your desired Globe products and services.

You have the right to be informed of the Personal Information that we collect, process, use, and share. We can provide you with such Personal Information, provided that such Personal Information does not amount to information deemed confidential or proprietary by Globe, or that your request for Personal Information is not vexatious or unreasonable.

You have the right to object or withhold your consent to the collection, processing, use, and sharing of your Personal Information. However, we may be constrained to terminate your Globe product or service as your Personal Information may be required to deliver such Globe product or service. Without your Personal Information, we will be unable to provide you with updates on Globe's latest offerings; similarly, you will be unable to participate in our events, promotions, or other activities.

[20] https://www.globe.com.ph/privacy-policy.html#gref

You have the right to suspend, withdraw, or order the blocking, removal, or destruction of your Personal Information in our processing systems upon discovery and substantial proof that your Personal Information is no longer necessary for the purpose or purposes for which it was collected, and for such other cases provided in the Data Privacy Act of 2012.

You have the right to seek indemnity for damages sustained, if any, due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of your Personal Information.
Should you feel that there has been mishandling or misuse of your Personal Information, or that any of your data privacy rights have been violated, you may email us at privacy@globe.com.ph.

3. Collection Of Customer Data

As part of our continuing relationship with you, we collect, process, use, and share your Customer Data in accordance with this Privacy Policy and the Terms and Conditions for the use of Globe products and services, as may be applicable.
The Customer Data that we collect, process, use, and share are either Personal Information or Non-Personal Information:

a. **Personal Information** is any information from which the identity of an individual can be reasonably and directly ascertained, or when put together with other information would directly and certainly identify an individual, such as name, gender, date of birth, address, telephone/mobile number, email address, proof of identification, etc. It also includes information about:
    I. The services provided to you, such as call/SMS details, location information, and certain information about your rate plans and features, as required by law;
    II. The location of your device whenever it is switched on, if you subscribe to location-based services, subject to coverage limitations; and
    III. Your use of our network, your Internet Protocol addresses, network performance experience, diagnostics, such as signal strength, dropped calls, data failures, and other network performance issues, to help us improve our network and quality of products and services, improve your user experience, determine tailored content, create new products and services, and for other legitimate business purposes.
b. **Non-Personal Information** is any information that does not identify you individually, and includes statistical or analytical data, and anonymized or aggregated reports.

4. Use Of Customer Data

a. We may share Customer Data with our subsidiaries, affiliates, partners, and third-party service providers as part of business operations and provision of products and services.
b. Without limiting the generality of the foregoing, Customer Data is used to, among others:
    I. Provide you with your subscribed products and services, including customer support;
    II. Help us improve our network and quality of products and services;
    III. Create new products and services;
    IV. Enhance your customer experience and determine tailored content to meet your preferences and needs;
    V. Communicate relevant services and/or advisories to you;
    VI. Abide by any safety, security, public service or legal requirements and processes;
    VII. Process information for statistical, analytical, and research purposes. The use of your information for statistical, analytical, and research purposes enables us to create anonymized and aggregated insight reports that we use to further improve your user experience and to provide new products and services;
    VIII. Create a customer portrait based on your demographic, and your behavioral, transaction, and interaction data across all products, systems, devices, and/or interaction channels, which we may use as a basis for sending you commercial and promotional alerts, personalized advertisements, financial service offers, and surveys. To be clear, should we need to share data with third parties for advertising and marketing purposes, we only share anonymized and aggregated data, and not your Personal Information;

IX. Compute for a telco score which may be shared with our subsidiaries, affiliates, partners and/or third parties, for various purposes such as, but not limited to, credit scoring, premium subscription offerings, product bundling, consistent with our goal to provide you with new products and relevant offerings to meet your changing needs; and

X. Comply with the requirements of the law and legal process, such as a court order; to comply with a legal obligation; or to prevent imminent harm to public security, safety, or order, collectively referred to as "Data Use Purpose."

When required by our Privacy Policy and the law, and before we collect, process, use, or share your Personal Information for any other purpose other than enumerated above, we will ask for your consent.

You may avail of our broadcast messages relevant to you through written correspondence, text messaging, internet, or other similar means of communication. You may also change your mind anytime and stop receiving them.

When you use our website and electronically communicate with us, depending on your settings, we may use cookies, web beacons, small data text files, or similar technologies to identify your device and record your preferences, with your consent. The completeness and accuracy of your Personal Information help us improve our products and services. Thus, we encourage you to update your Personal Information from time to time.

We outsource or contract the processing of Customer Data to third parties, such as but not limited to, vendors, service providers, partners, or other telecommunications operators, to fulfill any of the above purposes. They are only authorized to use Customer Data for such contracted purposes. They may have access to Customer Data for a limited time under reasonable contractual and technical safeguards to limit their use of such Customer Data. We require them to protect Customer Data consistent with our Privacy Policy.

During roaming or when availing of services offered by foreign service providers through our network, the storage, treatment, and transfer of your Personal Information may be subject to regulations different from Philippine regulations.

5. Protection Of Personal Information

We respect your privacy. We take paramount care in protecting your Personal Information. As such, we secure and protect your Personal Information with proper safeguards to ensure confidentiality and privacy; prevent loss, theft, or use for unauthorized purposes; and comply with the requirements of the law.

As Information Security threats continue to develop and evolve at such a rapid pace, we make reasonable and appropriate security arrangements and measures that use a variety of physical, electronic, and procedural safeguards to protect Personal Information. Globe runs a state of the art Security Operations Center with a dedicated team and personnel that monitors our network and systems to make sure risks to Globe and your Personal Information are properly managed. We regularly review our information collection, storage, and processing practices, including physical security measures, to guard against unauthorized access to our system and unauthorized alteration, disclosure, or destruction of information we hold.

We only permit your Personal Information to be collected, processed, used, and shared by our authorized employees, contractors, and subcontractors who hold such Personal Information under strict confidentiality and in accordance with their contractual obligations and who have implemented minimum security features against data leakage, unauthorized access, or disclosure. We restrict access to information to Globe employees, contractors, and subcontractors who need to know such information in order to process it for us, who are subject to strict contractual and technical safeguards, and who are accountable if they fail to meet these obligations.

We only give you or your authorized representative access to your Personal Information. We do not provide, sell, or share your Personal Information to anyone unless you have given your express consent. We also do not use nor share your

Personal Information with content and/or information providers without your prior request or consent. Personal Information will only be disclosed to third parties in accordance with this Privacy Policy.

We keep our records as accurate as possible. If your Personal Information is wrong, we give you ways to update it. Once you have registered as our customer, you may access your account details and correct your Personal Information by contacting Globe Customer Care ((+632) 7730-1000 or 211 using your mobile phone) or your relationship manager, as may be applicable; or by visiting any Globe Store or our website at www.globe.com.ph.

We keep your Personal Information in our business records, as may be applicable, while you are a customer, or as long as it is necessary to fulfill the purpose for which it was collected, or while it is needed by us for business, tax, or legal purposes. When disposing of your Personal Information, we take reasonable measures to ensure that it is done properly and is not accessible to the public.

We are not responsible for information, content, application, product, or service that we do not provide. But because we care for you and protect you, we take measures to fight spam, fraud, or any unauthorized messages that traverse our network. Further, we will not tolerate the use of our network that violates the law, which shall include but not be limited to:

a. Photo or video voyeurism, including the publication or broadcast or transmission through our network of any sexual act or any similar activity without the consent of the person involved and under circumstances in which the person has a reasonable expectation of privacy, is prohibited and unlawful with corresponding penalties under the law.
b. Child pornography is also prohibited and punishable by law and our network shall not be used in any manner for the storage, transmission, or dissemination of materials containing child pornography. We will report any instances of such activity that we become aware of, to the proper authorities as required by law.

We shall cooperate with law enforcement agencies to curtail criminality and prevent criminals from wreaking havoc over the internet, which shall include the blocking of certain sites or prevention of access to certain individuals, all in accordance with the stipulations of the law and with respect to legal due process.

6. High-Level Privacy Principles

In addition, we only want the happiest customers, so we commit ourselves to abide by Groupe Speciale Mobile Association (GSMA)'s high-level privacy principles based on internationally recognized and accepted principles on privacy and data protection as follows:

a. **Openness, Transparency, and Notice**
We are open and honest with you and will ensure that you are provided with clear, prominent, and timely information regarding our data privacy practices. We will provide you with information about the collection of your Personal Information, access, sharing, and further use of your Personal Information, enabling you to make informed decisions about whether to use a mobile application or service.
b. **Purpose and Use**
We will limit the access, collection, sharing, disclosure, and further use of your Personal Information to meet legitimate business purposes or to otherwise meet legal obligations.
c. **User Choice and Control**
We will give you opportunities to exercise meaningful choice and control over your Personal Information.
d. **Data Minimization and Retention**
We will collect, access, and use only the minimum Personal Information necessary to meet legitimate business purposes and to deliver, provision, maintain, or develop applications and services. Personal Information will not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations, and will subsequently be deleted or rendered anonymous.

e. **Respect User Rights**
You will be provided with information about, and an easy means to exercise, your rights over the use of your Personal Information.

f. **Security**
Personal Information will be protected, using reasonable safeguards appropriate to the sensitivity of the information.

g. **Education**
You will be provided with information about privacy and security issues and ways to manage and protect your privacy.

h. **Children**
An application or service that is directed at children will ensure that the collection, access, and use of Personal Information is appropriate in all given circumstances and compatible with applicable law.

i. **Accountability and Enforcement**
All responsible persons will be accountable for ensuring that these principles are met.

7. Contact Us

Should you wish not to:

a. Have your Personal Information disclosed or processed;
b. Receive marketing alerts and promotional messages from us, our subsidiaries, affiliates, and partners, you may immediately get in touch with us through our website at www.globe.com.ph or by contacting Globe Customer Care ((+632) 7730-1000 or 211 using your mobile phone).

For any questions or concerns, you may contact our Data Protection Officer as follows:

Data Protection Officer
Globe Telecom, Inc.
The Globe Tower
32nd Street corner 7th Avenue,
Bonifacio Global City, 1643 Taguig City,
Metro Manila, Philippines
Email: privacy@globe.com.ph

IJM