



Foundation for
Media Alternatives

PART II OF II

Gender and Privacy Online: Insights on the Philippines

JUNE 2020

Trigger warning: The following article includes accounts of sexual violence, which may be distressing for some readers.

Part 1 – Introduction

It was 2017. Maya (not her real name) was a development worker moonlighting as a talent for various video productions. A stranger had sent her a message request on Facebook to tell her that she was on a porn site. She verified the link referred to her and discovered that her photo had indeed been posted on a particular website, alongside another photo of a woman wearing white underwear.

In itself, her photo was quite innocuous. Most likely lifted from Facebook, it was an image of her speaking at an event where she was working as a photographer. Maya never wears white underwear, so she was a hundred percent sure the woman in the other photo was a different person. She would later find out the photo was actually posted on a number of other porn sites and was being spread around Facebook groups and chat groups dedicated to men who masturbate. Soon after, Maya started receiving on a regular basis harassing messages and dick pics from members of these groups.

Maya is a victim-survivor of online gender-based violence (OGBV), which is defined by the Association for Progressive Communications (APC) as “acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communications technologies (ICTs), such as mobile phones, the internet, social media platforms, and email”.¹ Her experience, which is a combination of harassment and impersonation (or identity theft), is just one of many manifestations of OGBV, which also include unauthorized access to accounts or devices, surveillance and stalking, and extortion, among others.

The Foundation for Media Alternatives, under the Take Back the Tech (TBTT) Philippines project, has been mapping OGBV cases since 2012. Last year (2019), TBTT recorded forty-nine (49) cases of OGBV in the Philippines, including offenses such as repeated harassment (25%), taking

¹ Association for Progressive Communications. (2015). From impunity to justice: Exploring corporate and legal remedies for technology-related violence against women. <https://www.genderit.org/onlinevaw>

photos/videos without consent (22%), and dissemination of the victims' private information (21%). Most of the time, they were committed using mobile phones (29%), through videos (25%), and online chats (15%) by someone known to the victim (73%). Almost half of the victims are aged 18-30 (49%), 42% are under 18, while 9% are 31-45 years old.²

Like offline modes of gender-based violence, the prevalence of OGBV in the country is deeply rooted in the country's patriarchal culture. Part I of this article on Gender and Privacy highlighted the notion that centuries of a patriarchal worldview have made Filipino notions and standards of privacy inherently unfair to women and members of the LGBTQIA+ community. This culture is further enabled by the convenience offered by online tools, as well as gaps in the existing legal framework. In this second installment, we take a closer look at gaps in the ways OGBV is addressed in the Philippines, particularly in relation to privacy, as well as possible ways forward.

² Foundation for Media Alternatives. (2020, March 9). *How do we fight online gender-based violence in the Philippines?* <https://www.fma.ph/2020/03/09/how-do-we-fight-online-gender-based-violence-in-the-philippines/>

Part 2 – OGBV laws and enforcement

There are a number of laws in place today that can be used to address OGBV. Outside of the Anti-Violence Against Women and Children Act (Republic Act No. 9262), the next most relevant is the Anti-Photo and Video Voyeurism Act of 2009 (Republic Act No. 9995), which penalizes the capture (without the consent of the subject), reproduction, publication, and distribution of sexual videos or images. And since OGBV usually involves the unauthorized use and/or disclosure of personal information, the country's Data Privacy Act of 2012 (Republic Act No. 10173) or DPA is also pertinent. Some of the prohibited acts under the DPA are the unauthorized processing of personal information and sensitive personal information (including photos or videos of sexual acts), processing of personal information for unauthorized purposes, malicious disclosure, unauthorized disclosure, and unauthorized access or intentional breach.

Despite having all these policies, however, enforcing them is consistently seen as a major challenge. When Maya first discovered that her photo had been posted online, she went to the National Bureau of Investigation's (NBI) Cybercrime Division to file a complaint. There, investigators informed her that because she did not know the perpetrator's identity, it would be difficult to pursue a case against that person. They then encouraged her to continue communicating with the individual to try and set up an entrapment operation. When she consulted a lawyer, the possible applicability of the DPA to her case was again brought up, but then she was still confronted with the same problem of having to identify the perpetrator.

Maya had to endure several weeks of trauma as a consequence of being in constant contact with her tormentor, with only the slightest hope that it would eventually lead to an apprehension. When the perpetrator (whose identity as one of her casual acquaintances and Facebook friends was all but verified at that point) finally agreed to meet for breakfast, Maya seized the opportunity and immediately reached out to the NBI agent assigned to her, hoping to set up an entrapment—only to be told that no agents were available since the expected meetup was scheduled on an early Sunday morning. Maya's heart sank.

Part 3 – Gaps in OGBV response

In 2014, FMA and APC published a research on the Philippine OGBV experience,³ wherein access to justice in the country was evaluated based on the existing legal framework. The report identified the anonymity of perpetrators as a major hurdle in prosecuting OGBV cases. It has now been more than five years and the challenge of attribution continues to persist.

In Maya's case, since the perpetrator was unidentified, she was immediately told that she did not have a strong case. The only way forward was for her to maintain contact with him until an entrapment operation could be set. The entire burden of identifying the person was placed squarely on her shoulders of her—the victim-survivor. It was a strategy that inevitably subjected her to more emotional and psychological trauma.

Maya's account also highlights a lack of sensitivity on the part of frontliners who deal with victim-survivors. When she sought help from the authorities, Maya was made to feel as if her case was not urgent or critical since she did not lose money like victims of online extortion or get violated physically. "Hindi ka naman na-ano" ("But you weren't physically assaulted"), they said. Statements like this demonstrate a remarkable lack of appreciation among many law enforcement officers of the gravity of OGBV offenses.

To be sure, the harms resulting from OGBV are plenty, varied, and are just as serious as those resulting from physical violence. With Maya, whenever she narrated her experience, she repeatedly mentioned how receiving unsolicited dick pics and inappropriate comments made her feel like she was being raped over and over. The reference is neither coincidence nor easy for her to make since she is, in fact, a rape survivor herself. She said the pain she felt every time someone sent her a dick pic on Facebook was every bit as painful as her harrowing past experience. It became exponentially worse when frustration set in after the entrapment she was expecting could not push through.

³ Garcia, L. and Manikan, F. (2014) *Gender Violence on the Internet: The Philippine Experience (Philippine Country Report on Technology-Related Violence Against Women in the Philippines)*.

Maya's case also confirmed another finding of the FMA-APC paper, which said that "in many cases, victims are discouraged [to file complaints] because the process is tedious and costly. Because of this, ...settling cases out of court has become an attractive option under the Philippine justice system".

In the end, Maya was left with no choice but to simply block her online tormentor.

Part 4 – OGBV and Privacy

Privacy and gender-based violence, whether online or offline, have always been intimately intertwined. Surveillance, which is arguably the most common privacy violation, is also seen as a form of violence that has been historically used as a patriarchal tool to control women’s bodies and sexuality.⁴ In their report on gender and privacy, Privacy International stress that, “[s]urveillance generates and magnifies power, and thus goes hand in hand with systems of oppression” such as patriarchy.⁵

Looking at the Philippine context, both technological and policy developments in recent years have certainly given rise to new dimensions of the privacy-OGBV correlation.

In 2014, the Supreme Court of the Philippines came out with a landmark decision on the bounds of online privacy in the case of *Vivares v. St. Theresa’s College*, which remains the instructional case today when appreciating a person’s reasonable expectation of privacy while using social media platforms. In its decision, the Court ruled that social media users cannot claim a reasonable expectation of privacy on an online social network (OSN) like Facebook, unless they post content under a “Me Only” privacy setting. To the Court, the duty-bearer when it comes to preserving online privacy are the users themselves, proclaiming that “self-regulation on the part of OSN users and internet consumers in general is the best means of avoiding privacy rights violations.”⁶

When the events that led to the *Vivares* case occurred in 2012, the DPA was just months away from becoming law. Unfortunately, it would take 4 more years, in 2016, before the National Privacy Commission (NPC)—the government body mandated to administer and implement the law—was established. Since it began its operations, the Commission has dealt with various data breaches and pressing privacy-related issues such as the country’s COMELEAK scandal and Cambridge Analytica fiasco, which both rattled the globe. As of the time of this writing, though, it has yet to come up with

⁴ Shephard, N. (2017) *What is Sexual Surveillance and Why Does It Matter*. <https://www.genderit.org/feminist-talk/what-sexual-surveillance-and-why-does-it-matter>

⁵ Privacy International. (2018, November). *From Oppression to Liberation: Reclaiming the Right to Privacy*. <https://privacyinternational.org/sites/default/files/2018-11/From%20oppression%20to%20liberation-reclaiming%20the%20right%20to%20privacy.pdf>

⁶ G.R. No. 202666, September 29, 2014

any official statement, issuance, or resource material on the problem of non-consensual sharing of intimate images, or any gender-related issue.

Then, there is the issue of anonymity, which is a polarizing aspect of privacy. Since a major hurdle in the investigation and prosecution of OGBV cases is identifying the perpetrators who usually maintain anonymous online personas, there has been a longstanding debate on whether stripping online users of anonymity (e.g., through a real-name policy) would be an effective solution. Those in Privacy International offer an alternative perspective. In *From Oppression to Liberation: Reclaiming the Right to Privacy*, they state:

Online harassment is a privacy issue: every time a woman, trans and gender diverse person is harassed, it is their personal space and boundaries that are invaded and violated, even when it takes place on what is perceived as a public platform. This understanding of online harassment shows the need for an understanding of privacy that is broad and encompassing for women, trans and gender diverse people, as patriarchy relies on those privacy violations to enforce its power.⁷

This frame of thinking allows for a view of privacy as being instrumental to human freedom and dignity, rather than a tool for avoiding liability.

⁷ Privacy International, *supra*.

Part 5 – What should be done?

Very little has changed since the FMA-APC study in 2014. A cursory review of the many cases being reported to TBTT Philippines (including Maya's) suggests that the report's recommendations then are just as valid and appropriate today.

The government must strictly implement laws related to OGBV, develop effective mechanisms for reporting and service referral, and allocate adequate resources for personnel tasked to investigate cybercrimes. There is also a need to review policies that could even be inflicting harm on victims of online sexual violence, such as the cybersex provision of the Philippines's anti-cybercrime law.

Digital platforms and other internet intermediaries play a major role in the prevalence of OGBV and should therefore be more proactive themselves in addressing it. The 2019 figures from TBTT Philippines show that of the 49 cases recorded, 29% were committed with the use of mobile phones, and 15% were committed through online chats. 22% of the cases involved the use of Facebook, in particular. This underscores the importance of Facebook's close coordination and cooperation with both government and civil society actors to come up with solutions that uphold people's rights and safety within its platform and other applications.

Institutions like schools have also emerged as key actors in the push for behavioral changes, especially among young people. This is a timely development considering that, as per TBTT's records, young people are the most at-risk group when it comes to OGBV. Maya herself observed that the account that posted her photo online also did the same to other girls that were much younger than her. Some of them were probably still in grade school. This is consistent with the trend of non-consensual sharing of intimate images among young students cropping up more frequently in the Philippines in recent years.⁸

⁸ Domingo, K. (2019, May). 'Pisay students seek grad ban for 6 seniors over nude photo upload.' *ABS-CBN News*. <https://news.abs-cbn.com/news/05/23/19/pisay-students-seek-grad-ban-for-6-seniors-over-nude-photo-upload>

Meanwhile, the spike in incidents involving scandalous online groups and pages⁹ and the emergence of a “callout culture” have also brought up the need for clearer guidelines in dealing with digital evidence, especially those posted anonymously in online platforms and without the consent of the people involved. Authorities need to find a way so that materials uploaded or posted online can be used to deliver justice for victims of online harassment without unnecessarily infringing on privacy rights and other civil liberties.

Today, unwarranted surveillance and invasions of privacy are still being used constantly as tools to uphold the archaic and discriminatory concept of patriarchy. This means the real fight remains to be the complete dismantling of the systems of oppression that have long placed women and sexual minorities in cycles of violence. Unless these causes of OGBV are uprooted, regardless of legal and technical safeguards, the perpetrators of these crimes will always find ways to weaponize technology and navigate the boundaries of privacy rights, motivated solely by their self-interest.

That said, it is also important to emphasize that OGBV (and gender-based violence in general) is a far more complicated issue than just violence experienced by women. It also intersects with other forms of systemic oppression such as transphobia. Other recent local cases, such as that of a female filmmaker catfishing and orchestrating the sexual abuse of a trans woman¹⁰, demonstrate that women can be perpetrators of gender-based violence as well.

With so many challenges to hurdle, many victim-survivors, in the meantime, are effectively left to fend for themselves, weighed down by the disappointment and distrust the government itself has caused and nurtured. Some become desperate enough and try to assert their rights in their own unique ways. Take Maya who, before completely cutting off her communication with her tormentor, warned the

⁹ In 2017, a trend of “*Hokage*” Facebook groups and group chats was revealed to be prevalent among Filipino men. These secret groups were used as a platform to share intimate photos and videos of women usually taken or shared without consent. In 2020, another batch of [Filipino Facebook groups and pages](#), this time focusing on child pornography, gained public attention.

¹⁰ Pascual, J. (2020, April). ‘The Sam Morales story isn’t just a catfishing story – it’s a portrait of transphobia in the Philippines.’ *ANCx*. <https://www.gmanetwork.com/news/hashtag/content/616746/pastor-hokage-fb-groups-trading-lewd-photos-of-women-exposed/story/>

latter that if he does anything to her again, she would contact a gun-for-hire to hunt him down. In her interview, she insists she is serious about her threat. In her mind, guns-for-hire these days, along with the type of vigilante justice they offer, present a more realistic and reliable option than law enforcement in the eyes of someone seeking true closure and relief.



About FMA

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

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

FMA seeks to develop programs and projects that strategically address the questions of access to and equity of disadvantaged sectors in the area of information and communications—and in locating the so-called digital divide within existing socio-political divides, including gender.