HUMAN RIGHTS AND THE PHILIPPINE DIGITAL ENVIRONMENT JOINT SUBMISSION TO THE UNIVERSAL PERIODIC REVIEW OF THE PHILIPPINES

For consideration at the 41st session of the UPR Working Group

March 2022

I. Introduction

1. The Foundation for Media Alternatives (FMA)[1] welcomes the opportunity to contribute to the fourth cycle Universal Periodic Review (UPR) of the Philippines. FMA is submitting this report jointly with the Association for Progressive Communications (APC)[2], Access Now[3], and the Women's Legal and Human Rights Bureau (WLB).[4]

2. This submission[5] focuses on the Philippines' compliance under international human rights law on the promotion, protection and fulfillment of rights particularly in the Internet, and observes the following areas of concern:
   - Freedom of expression
   - Online gender-based violence;
   - Privacy and data protection

---

1 FMA is a non-profit organization based in the Philippines that works on the intersection of human rights and information and communications technology (ICT).

2 The Association for Progressive Communications (APC), an organization in consultative status with ECOSOC, advocates the strategic use of information and communications technologies to advance human rights. The APC network has 62 organizational members and 29 individual members active in 74 countries, including The Philippines. https://www.apc.org

3 Access Now is an international organization that works to defend and extend the digital rights of users at risk around the world. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organization, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age.

4 WLB is a feminist legal non-governmental organization based in the Philippines.

5 Apart from the submitting organizations, FMA also wishes to acknowledge Privacy International for their valuable inputs to this report.

3. The previous UPR made no mention of the right to privacy, nor of any privacy-related violations in the country. However, privacy issues, including State surveillance and data breaches have become more prominent since the last UPR.

4. The Philippine government supports taking action to promote gender equality and eliminate discrimination, as well as coming up with policies to eliminate violence against women, children, and LGBTI persons. However, various forms of violence against women, children and LGBTI persons continue, especially in the digital sphere. While the government supports measures to enable women to have effective access to the justice system, and capacity-building on gender-sensitive handling of victims of trafficking, women survivors still complain of gender insensitivity of law enforcers and their use of age-inappropriate questions, thus making access to justice for women and girl children more difficult.

5. The Philippine government also took note of recommendations to take necessary measures for the protection of freedom of opinion and the promotion of media freedom and the rights of journalists, as well as adequate protection for human rights defenders and journalists in the previous UPR. These are rights enshrined in the United Nations (UN) Universal Declaration of Human Rights (UDHR) and the Philippine Constitution, but media workers and journalists continue to face harassment and red-tagging for being critical of the administration.

II. Legal Framework

6. The Internet was first introduced in the Philippines in 1994 and since then the number of Filipinos connected has increased exponentially. In 2022, it is estimated that 68% of the total Philippine population of about 111.8 million (or about 76 million Filipinos) are online.[6]

7. Laws and policies pertaining to the Internet have been enacted to address new developments, especially in relation to technology. Some of these laws include, among others, the E-Commerce Act of 2000 (RA 8792), the Anti-Child Pornography Act of 2009 (RA 9775), the Anti-Photo and Video Voyeurism Act of 2009 (RA 9995), the Data Privacy Act of 2012 (RA 10173), the Cybercrime Prevention Act of 2012 (RA 10175), the Expanded Anti-Trafficking in Persons Act of 2012 (RA 10364), Department of Information and Communications Technology Act of 2015 (RA 10844), Safe Spaces Act of 2019 (RA 11313), the Telecommuting Act (RA 11165), and the Anti-Terrorism Act of 2020 (RA 11479).

8. The Department of Information and Communications Technology (DICT) was established in 2016 by virtue of Republic Act 10844 as the "primary policy, planning, coordinating, implementing, and administrative entity of the Executive

[6] Simon Kemp. Digital 2022: The Philippines. February 15, 2022, https://datareportal.com/reports/digital-2022-philippines

Branch of the government that will plan, develop, and promote the national ICT development agenda." Attached to the DICT are the National Privacy Commission (NPC), also established in 2016, the National Telecommunications Commission, and the Cybercrime Investigation and Coordinating Center (CICC).

9. The country adopts generally accepted principles of international law as part of the law of the land. A Bill of Rights is enshrined in the 1987 Philippine Constitution and promotes the rights of all individuals as embodied in the UDHR. The Philippines is a long-time member of the UN (since 1945) and has ratified nine of the ten core international human rights instruments.[7] Accordingly, it is duty-bound to observe the rights laid down in such international legal instruments.

III. Philippine Compliance with Its International Human Rights Obligations

10. The Internet today has become a space where individuals can express their freedom of speech and expression, as enshrined in Article 19 of the UDHR and the International Covenant on Civil and Political Rights (ICCPR). As former UN Special Rapporteur Frank La Rue once said, the internet has become an "enabler" of rights.[8] It has become this new environment that constantly evolves, in stride with various technological advances. For many, it remains an uncharted terrain, especially in the realm of law, policy and governance. This has sometimes resulted in confusion amidst unfamiliar contexts, as ICTs and the Internet may be used both to advance human rights, or to enable violations of these same rights.

11. Human rights are universal, indivisible, interrelated, and interdependent. Every person has inherent rights no matter where one is, even in the realm of cyberspace. Activities that are done online or in digital spaces may seem virtual, but they are also very real. Therefore these same rights that people have offline must also be protected online. This was established via UN Human Rights Council (HRC) Resolution 20/8 in June 2012. Follow-up HRC resolutions on the enjoyment of human rights and the Internet in 2014, 2016, 2018, and 2021,[9] as well as HRC and UN General Assembly Resolutions on the right to privacy in the digital age expanded on this fundamental principle.

Given these international standards and national constitutional and statutory mandates, the following areas of concern are raised:

---

[7] The Philippines did not sign, nor has it ratified the Convention for the Protection of All Persons from Enforced Disappearance.

[8] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue A/HRC/17/27

[9] UNGA Resolution 36/… in 2016, 38/7 in 2018, and 47/16 in 2021 on the promotion, protection and enjoyment of human rights on the Internet.

Freedom of expression

12. Libel is being decriminalized by many States.[10] The UN Human Rights Committee, in a communication to the Philippine government declared that libel is "excessive" and "incompatible" with the ICCPR, which the country ratified in 1986, and recommended that "States parties should consider the decriminalization of defamation and, in any case the application of criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty."[11] Libel in some cases is used to hinder freedom of expression, often to silence investigative journalists, potential whistleblowers, or any person deemed to be expressing dissent to the existing regime.

13. Article III Section 4 of the Philippine Constitution of 1987 states that "No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances." However, the crime of libel or defamation has been used as a means to suppress freedom of expression and freedom of the press in the Philippines. Cases of government officials and influential people filing cases against the media have produced a chilling effect and could lead to self-censorship. For instance, the Secretary of the Department of Energy filed libel complaints against reporters, editors, and executives of Rappler, ABS-CBN, Business World, Philstar, Manila Bulletin, GMA News Online, and Business Mirror for publishing a story on him and Duterte campaign supporter Dennis Uy on the disputed buyout of the Malampaya gas field.[12] The fear of imprisonment or the imposition of fines has prevented the more cautious media outlets from criticizing government officials.[13]

Cyberlibel

14. Libel found its way into the Cybercrime Prevention Act of 2012. Section 4(c)4 of the said Act defines cyber libel as "the unlawful or prohibited acts of libel as defined in Article 355 or the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future."

---

[10] CCPR General Comment No. 34 of July 2011. Available in https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2bWPAXiks7ivEzdmLQdosDnCG8FaJ7cpkH%2fR9YlpwV%2bAPs%2bmcFvCdQgiL4iR9ZkL7Bv4oc2QLZ3AWYcNmMYP3SjhOMZ9

[11] Alexander Adonis vs. The Philippines, Communication No. 1815/2008, U.N. Doc. CCPR/C/103/D/1815/2008/Rev.1(2012). Available in http://hrlibrary.umn.edu/undocs/1815-2008.html

[12] Lian Buan, "Cusi sues Rappler, 6 other news orgs for libel over Malampaya-Dennis Uy reports," Rappler, December 3, 2021, https://www.rappler.com/nation/cusi-sues-rappler-other-news-organizations-libel-malampaya-dennis-uy-reports/

[13] Sheila S. Coronel, "A 'Fraught Time' for press freedom in the Philippines," NPR, January 17, 2018, https://www.npr.org/sections/parallels/2018/01/17/578610243/a-fraught-time-for-press-freedom-in-the-philippines

Further, punishment of online libel under RA 10175 is one degree higher than offline libel, effectively decreeing heavier sanctions for "cyberlibel". The Supreme Court has ruled that commission of existing crimes through the internet should be considered as a qualifying circumstance. It ruled that in using this technology, "*the offender often evades identification and is able to reach far more victims or cause greater harm".*[14] This has been contested by human rights observers - noting, as with criminalization of defamation offline, that criminal penalties for apparent libel online are also overbroad and will disproportionately impact on the right to freedom of expression and information. It has been used continually to silence journalists, bloggers, and ordinary Internet users. One landmark case of cyber libel in the Philippines is that of Maria Ressa and Reynaldo Santos, Jr., who were convicted of the crime in 2020 for the republication of an article on the late Supreme Court chief justice Renato Corona's links to businessmen, including Wilfredo Keng. Ressa and Santos could face up to six years in prison, a verdict that sets "an extraordinarily damaging precedent" for press freedoms.

Cyber attacks on websites of media and human rights groups

15. Several incidents of cyber attacks, such as defacement of websites and distributed denial of service (DDoS) attacks,[15] against the media and human rights groups have been recorded in the last few years. In 2019, alternative media groups Altermidya, Kodao Productions, and Pinoy Media Center filed a civil case[16] against groups and individuals believed to be behind the cyberattacks on their websites. The defendant-companies claimed that they had no prior knowledge that their cyber-infrastructure was being used for these attacks. The alternative media groups withdrew the case subject to the defendants' commitment to support a free press to establish effective mechanisms to combat such attacks.[17]

16. The continued cyber attacks against independent media outlets and the civil society alliance Karapatan may be linked to their independent media reporting and human rights advocacy, respectively. These cases were investigated by the Swedish-based digital forensics nonprofit Qurium Media, who found that the attacks were linked to the Department of Science and Technology (DOST) and the

---

[14] Disini et. al. v. Secretary of Justice, et. al., G.R. No. 203335, February 11, 2014 and other cases consolidated in this decision.

[15] DDoS is a malicious attempt to bring down a website by flooding it with an overwhelming amount of simulated traffic. It is a form of system interference that is illegal in the Philippines under the e-Commece Act of 2000.

[16] Jannes Ann J. Ellao, "Alternative media submit evidence vs IT companies over cyber attacks," Bulatlat, September 9, 2019, https://www.bulatlat.com/2019/09/09/alternative-media-submit-evidence-vs-it-companies-over-cyber-attacks/

[17] Altermidya, "Parties to cyberattacks case reach agreement", February 24, 2020, https://www.altermidya.net/parties-to-cyberattack-cases-reach-agreement/

Philippine military.[18] The Computer Emergency Response Team - Philippines (CERT-PH) of the DICT also confirmed that an Internet Protocol address linked to cyberattacks against alternative media outfits is assigned to DOST and the military.[19] The DOST said that the allegations were "unfounded and patently false."

17. The news websites of Rappler and ABS-CBN, as well as the websites of Vera Files, GMA News, and CNN Philippines, have all experienced several technical attacks in recent months.[20] A hacking group called Pinoy Vendetta claimed responsibility for these attacks, as well as for the attacks on the websites of opposition senators, the Philippine Senate, and left-leaning groups. The spokesperson of the National Task Force to End Local Communist Armed Conflict (NTF-ELCAC), Lorraine Badoy, praised this hacking group for being able to put the websites of leftist groups down, but the NTF-ELCAC and Pinoy Vendetta have consistently denied that they have a working arrangement.[21]

Red-tagging

18. "Red-tagging" or the labelling of individuals and groups as communists or terrorists without substantial proof of any unlawful conduct is a serious threat to civil society and freedom of expression in the Philippines.[22] The NTF-ELCAC, established by the Duterte administration in December 2018, has consistently been red-tagging activists, human rights defenders, and journalists critical of the government through its social media posts and official pronouncements.[23] Authorities also conduct raids against groups or individuals, planting evidence that can be used to bring charges against them, which is especially dangerous given the passage of the Anti-

---

[18] See https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26662

[19] Rappler, "Highest Gov't Body for Cybersecurity Confirms AFP Link to Cyberattacks – Targeted Sites," Rappler, September 24, 2021, https://www.rappler.com/technology/qurium-cert-ph-confirms-afp-link-cyberattacks-bulatlat-altermidya

[20] Gemma B. Mendoza, "Heightened DDoS attacks target critical media," Rappler, December 24, 2021, https://www.rappler.com/technology/cyberattacks-abs-cbn-rappler-vera-files-similar-signatures/

[21] Gelo Gonzales, "Hacker group mounts DDoS attacks vs PH news outlets, hailed by gov't," Rappler, February 24, 2022, https://www.rappler.com/technology/ntf-elcac-ddos-attacks-endorsement/

[22] See, generally, UN Human Rights Council, Situation of human rights in the Philippines, UN Doc A/HRC/44/22, June 29, 2020 (A/HRC/44/22), citing Dissenting opinion of Associate Justice Leonen in Carlos Isagani Zarate et. al. case, Supreme Court, November 10, 2015.

[23] "Philippines: End Deadly 'Red-Tagging" of Activists," Human Rights Watch, January 17, 2022, https://www.hrw.org/news/2022/01/17/philippines-end-deadly-red-tagging-activists

Terrorism Act of 2020.[24] Such practices put individual lives at risk and have resulted in the death of some activists, as in the cases of human rights advocate Zara Alvarez and Anakpawis Chairperson Randy Echanis.[25]

19. Philippine law prescribes a process for designating individuals and organizations as terrorist organizations. Pursuant to Republic Act No. 11479 ("The Anti-Terrorism Act of 2020"), the Anti-Terrorism Council (ATC) issued:

    - Resolution No. 16 (2021): Designation of individuals affiliated with the local terrorist groups, which were designated under Anti-Terrorism Council Resolution No. 13 (2020), as terrorists.[26]
    - Resolution No. 17 (2021): Designation of Central Committee Members of the Communist Party of the Philippines and the New People's Army also known as Bagong Hukbong Bayan (CPP/NPA), which was designated under Anti-Terrorism Council Resolution No. 12 (2020), as terrorists.[27]

    Despite the fact that these resolutions contain the list of individuals officially designated as terrorists, government officials continue to redtag human rights defenders who are not on these lists and without due process.

20. The lawyers of those listed in Resolution No. 17 (2021) said that the Resolution was a blatant violation of their clients' right to due process, citing the fact that the Manila Regional Trial Court had already previously removed their names from a similar petition in 2018 for lack of evidence linking them to terror acts.[28] In January 2022, the ATC named 16 organizations linked to the Communist Party of the Philippines as terrorist groups.[29]

---

[24] Bella Perez-Rubio, "After Human Rights Day arrests, HRW says there is 'damning history' of cops planting evidence", Philstar.com, December 12, 2020, https://www.philstar.com/headlines/2020/12/12/2063300/after-human-rights-day-arrests-hrw-says-there-damning-history-cops-planting-evidence; Al Jazeera, "'Appalled': UN urges probe into killing of Philippine activists," Aljazeera, March 10, 2021, https://www.aljazeera.com/news/2021/3/10/un-urges-probe-into-killings-of-philippine-activists; Reporters without borders, "Filipina journalist arrested for firearms planted by police," RSF, December 15, 2020, https://rsf.org/en/news/filipina-journalist-arrested-firearms-planted-police

[25] International Commision of Jurists. Danger in dissent: Counterterrorism and human rights in the Philippines. January 2022, https://www.icj.org/wp-content/uploads/2022/01/ICJ_PhilippinesRedTagging_270122.pdf

[26] https://drive.google.com/file/d/1UBybEW1UO9x5bS-0lMFa-CNtZdCQUDRT/view

[27] https://drive.google.com/file/d/1SUxje-6cbH73RM1RPhYGG2gwWdgCrBat/view

[28] Dona Z. Pazzibugan and Krixia Subingsubing, "Red-tagging at its finest," Inquirer.net. May 14, 2021, https://newsinfo.inquirer.net/1431638/red-tagging-at-its-finest

[29] Benjamin Pulta, "16 organizations linked to Reds designated as 'terror groups'," Philippine News Agency, February 23, 2022, https://www.pna.gov.ph/articles/1168356

21. The Supreme Court, in a decision promulgated on December 7, 2021, ruled that the ATC's power to designate terrorist individuals, groups of persons, organizations, or associations upon finding of probable cause, is constitutional.[30]

22. This pattern of red-tagging becomes even more dangerous given the context of extrajudicial killings in the country under the Duterte administration. The United Nations in 2018 reported the alarming level of reprisals and intimidations in 38 countries, including the Philippines. In 2019, the Human Rights Council adopted resolution 41/2 requesting the High Commissioner to prepare a report on the human rights situation in the Philippines. The 2020 report confirmed the widespread and systematic killings and arbitrary detention in the context of the war on drugs, killings and abuses targeting farmers and indigenous peoples, the silencing of independent media, critics and the opposition, and called on the Human Rights Council to "establish an on-the-ground independent, impartial investigation into human rights violations in the Philippines."[31]

Freedom of expression and sexual rights

23. Section 4(c)1 of Republic Act 10175 or the Cybercrime Prevention Act of 2012 is overly broad and vague. It defines cybersex as *"the willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration."*

24. Neither the law, nor its implementing rules and regulations, defines what a "lascivious exhibition" is or what "sexual organ or sexual activity" are. The law does not even clarify whether works of art that depict nude individuals, sold in whatever form or posted on the internet, would fall under this category. The very wording of the provision may therefore "empower law enforcers to pass off their very personal standards of their own morality," according to the dissenting opinion of one Associate Justice of the Supreme Court.[32]

25. Women's groups in the Philippines have long criticized the aforementioned cybersex provision in the law as being *"anti-women, focusing on 'criminalization, unmindful of its possible effects and without clear understanding of the inherent nature and characteristics of ICTs relating to violence committed against women"*. Rather than recognize a person's agency to express sexuality online, it

---

[30] G.R. No. 2522578.

[31] "Philippines" Human rights experts renew call for an on-the-ground independent, impartial investigation," OHCHR, June 25, 2020, https://www.ohchr.org/en/press-releases/2020/06/philippines-un-human-rights-experts-renew-call-ground-independent-impartial?LangID=E&NewsID=25999

[32] Disini v. Secretary of Justice, G.R. No. 203335, February 18, 2014, Dissenting and Concurring Opinion (leonen J.), http://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/56650

criminalizes such online behavior.[33] The provision fails to consider issues of anonymity, affirmation and the fluidity of online identity - how technology allows people to move beyond the usual social markers of class, ethnicity, gender, and age and how technology fulfills a need to express oneself online, as an alternative to oppressive offline spaces.[34]

Online Gender-Based Violence

26. Violence against women (VAW) is a manifestation of historically unequal power relations and systemic gender-based discrimination. It is a human rights violation under the Convention on the Elimination of All Forms of Discrimination and other international human rights instruments to which the Philippines is a signatory.

27. The rapid development of technology has given rise to different and new manifestations of VAW. Online VAW extends to "any act of gender-based violence against women against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately."[35]

28. Cases of online gender-based violence (OGBV) in the Philippines are continuously rising, especially during the height of the COVID-19 pandemic, despite initiatives from the government.[36] From 2012 to 2021, FMA was able to map 579 cases of OGBV in the Philippines.[37] At the height of the COVID-19 pandemic in 2020,

---

[33] Women's Legal and Human Rights Bureau, "Delete, Undo, Retrieve: Statement on the cybercrime prevention act of 2012,"GenderIT.org, October 10, 2012 https://genderit.org/feminist-talk/delete-undo-retrieve-statement-cybercrime-prevention-act-2012

[34] FMA stakeholder consultation on cybersex, 7 June 2019.

[35] Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective to the UNHRC in 2018 https://digitallibrary.un.org/record/1641160?ln=en

[36] The rising cases of VAW during the pandemic triggered various initiatives and updates from the government. The Philippine Commission on Women (PCW) and other government agencies activated and promoted hotlines online where women can report cases of abuse, including during the lockdown period. The Commission on Human Rights launched an online website where people can report incidents of gender-based violence during the lockdown period, including online harassment#. The Enhanced 911 National Emergency Hotline was updated to accommodate and respond to calls regarding incidents of violence against women and children (VAWC).# This was the result of a joint memorandum circular by the Department of the Interior and Local Government, the Department of Social Welfare and Development, and the Department of Justice. The National Mental Health Crisis 24/7 Hotline was also launched to help provide mental health crisis intervention and counseling services.

[37] Cases were sourced from media reports by FMA and mapped using the Take Back the Tech! platform. Incidents were also mapped from inquiries received by the Facebook pages of FMA, Women's Rights Online Philippines, and Take Back the Tech! Philippines.

OGBV incidence rose to 165%,[38] which follows the consistent findings of increased gender-based violence in times of crisis. The most prevalent cases in 2020 were taking photos/videos without consent (40.77%), sharing and/or disseminating private information (33.85%), and abusive comments (28.46%). Platform providers have also been reported to have contributed to aggravating women's experiences of online abuse.[39]

29. FMA's 2021 year-end report on OGBV include the following findings:

    - Mobile phones (86.67%) are the most commonly used devices followed by social media platform Facebook (25.33%). Online messaging platforms (21.33%) and videos (21.33%) were also among the ICT used.
    - OGBV was mapped in social networking sites other than Facebook (13.33%) such as Instagram, TikTok, and dating applications. Other devices and platforms (13.33%) such as Zoom and photo editing applications were also used in the perpetration of OGBV.
    - Survivors face emotional harm (80.00%), sexual harm (49.33%), and harm to reputation (37.33%). Physical harm (25.33%) is also present notably in trafficking cases involving ICTs.
    - The perpetrator is often a stranger to the victim-survivor (58.67%). However, in almost half of the cases, they are someone familiar to or known by the victim-survivor (49.33%). Groups of people were also indicated as perpetrators in 44% of the reports.

30. Based on the reported cases received by the WLB from June 2020 – February 2021,[40] 37% of OGBV cases involve girls below 18 years old, while 47% involve students. Their common complaints are sex videos and nude photos circulated mostly when they were minors. Some of these cases were reported to the police but due to its nature, online gender-based violence is often trivialized, especially when there is no physical violence involved.

---

[38] Based on the cases mapped by FMA for the period covering January to December 2020. Available at https://fma.ph/2021/02/19/online-gender-based-violence-in-the-philippines-our-year-end-round-up-report/

[39] For example, Google Drive has been flagged by women's groups for the publicly accessible links containing nude images of women being circulated without women's consent.

[40] Actual documented cases of WLB during the height of the pandemic.

31. Despite the recent passage of Republic Act 11313 or the Safe Spaces Act,[41] reporting OGBV cases online remains a challenge, and taking down nude photos and sex videos appears to be even more difficult. Victims are still left in the dark as to what kind of evidence should be preserved and presented in court. Some of the survivors who approached WLB also complained about gender insensitivity and the use of age-inappropriate questions by cyber experts in law enforcement, thus making access to justice for women and girl children more difficult.

The right to privacy

32. Privacy is a fundamental human right enshrined in numerous international human rights instruments[42] such as the UDHR and the ICCPR. Restrictions on the right can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[43] The Philippines adopts generally accepted principles of international law as part of the law of the land.[44] Accordingly, as a signatory to the UDHR and a number of human rights treaties, including the ICCPR, it is duty-bound to observe and uphold the right to privacy.

33. The 1987 Constitution of the Philippines also protects citizens against unreasonable searches and seizures and renders inviolable the privacy of their communication and correspondence. The Bill of Rights provides:

> *SECTION 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any*

---

[41] Republic Act No. 11313 or the Safe Spaces Act was passed in 2019 to expand the scope of the Anti-Sexual Harassment Act of 1995 or R.A. 7877. The law recognizes gender-based online sexual harassment which is defined as *"any online conduct targeted at a particular person that causes or is likely to cause another mental, emotional, or psychological distress, and fear of personal safety."* These sexual harassment acts include unwanted sexual remarks and comments, threats, uploading or sharing or one's photos without consent, cyberstalking and online identity theft.

[42] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[43] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[44] 1987 Constitution, Article II, §2.

purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

SECTION 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

(2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.

Privacy impact of government COVID-19 response

34. When the COVID-19 pandemic was declared in March 2020, the Philippine government engaged in contact tracing efforts to monitor and contain the spread of the coronavirus. However, poor leadership, ineffective regulation, and a general lack of coordination among government agencies, including local government units, resulted in the creation of multiple contact tracing systems, many of them via digital applications.[45] With little to no screening process involved, the government created multiple databases that have shown little use to date, while exposing the personal data of millions of Filipinos to a heightened risk of unauthorized use and exposure.[46]

35. When contact tracing applications were deployed, several concerns were disclosed and it remains unclear if, in the process of addressing these concerns, data already disclosed to contact tracing companies have been protected.[47] One application was described as “borderline spyware” because apart from collecting personal data, it also required permissions to use the phone camera and microphone, access contacts,and location, and read messages and access

[45] Some of the examples are StaySafe.ph, COVID Kaya, Traze, Tanod Covid, Trace Together, Kontra COVID. See Senate Economic Planning Office, “COVID-19 Response: Strengthening Contact Tracing”, May 2021, https://legacy.senate.gov.ph/publications/SEPO/Policy%20Brief_COVID-19%20Response,%20Strengthening%20Contact%20Tracing.pdf.

[46] Foundation for Media Alternatives. A Pandemic as Vector for Surveillance and Other Abuses. Available at https://fma.ph/wp-content/uploads/2021/09/WASP-report-final.pdf

[47] Digital Reach, Digital Contact Tracing in Southeast Asia The SummaryReport Submitted to the United Nations Special Rapporteur on the Right to Privacy Prof. Joseph Cannataci”, December 8, 2020, https://digitalreach.asia/wp-content/uploads/2020/12/Report-Submitted-to-SR-on-Privacy-FINAL.pdf

external storage.[48] It also remains unclear if the private companies providing contact tracing services are being monitored on their obligation to delete personal data or information after the agreed period.

Government measures facilitating mass state surveillance

36. With increasing reports of attacks against private citizens and legitimate organizations, it is important to assess existing laws and programs that the government is implementing and that may facilitate mass state surveillance against citizens. We highlight here the emerging threats from various pieces of legislation.

- ***Anti-Terrorism Act of 2020.*** Despite 37 petitions against its constitutionality, the Supreme Court upheld the constitutionality of the Anti-Terrorism Act of 2020, except for two contested provisions. In its current state, the law still features provisions prone to abuse, including those that may potentially be used by the government to engage in illegal and/or mass surveillance. Among them, Section 16 stands out because it facilitates the surveillance even of individuals merely suspected of specified crimes sans a search warrant and without having to prove that other effective means of collecting evidence are unavailable or impossible. The law also expressly provides that telecommunications service providers may be compelled to produce all customer information, identification records, content data, and even metadata.
- ***Philippine Identification System (PhilSys) Act (Republic Act No. 11055).*** Enacted in 2018,the PhilSys Act has inherent vulnerabilities and features susceptible to government abuse. Function creep is built into the system since the law allows for the expansion of use cases through the mere issuance and subsequent amendments of implementing rules. The law also fails to provide a cap on the amount of biometric information that may be collected by the government, and leaves the door open to the consolidation of various government ID systems that could increase exponentially all attendant risks. It also facilitates data surveillance as it requires the retention of a person's record history (i.e., log of all instances an individual uses his or her PhilID). Embedded safeguards are nondescript, with proponents relying heavily on the country's data protection law as a deterrent to any potential data breach or malfeasance.
- ***Executive Order No. 112***. On December 15, 2020, the government went ahead with its plan to implement measures pertaining to the processing of Advance Passenger Information and Passenger Name Record data via an administrative issuance by the Office of the President. Such measures fall short of the country's obligations under the ICCPR, most notably those relating to the right to privacy. The Philippine legal framework is also inadequate to ensure that the processing of said data does not lead to privacy violations.
- ***The proposed SIM Card Registration Act*.** The proposed law was ratified by the House of Representatives and the Senate on February 2, 2022, and, if not

[48] "House probe eyed on gov't-backed contact tracing app", CNN, July 2, 2020, https://www.cnnphilippines.com/news/2020/7/2/House-probe-StaySafe-contact-tracing-app.html

signed or vetoed by President Duterte, will lapse into law on April 16, 2022. It seeks to build another massive database that immediately presents itself as a major security risk. If established, such database would add itself to the Philippine government's growing list of data repositories, which, in the wrong hands, could serve as potent tools for mass surveillance and authoritarianism, especially when coupled with other draconian measures such as the controversial Anti-Terrorism Act. To make matters worse, it will become a premium target for malicious actors who will surely seek access to and try to profit from its content through inappropriate use or its sale to moneyed interested parties.The potential for abuse and function creep is high, especially when it comes to the use of the registration information for surveillance, owing to the bill's vague scope, ambiguous provisions, and insufficient legislative guidelines. Meanwhile, the system would afford the government easy access to the data collected while providing little to no limitation on its use.

Subpar implementation of data protection law

37. Despite the existence of the Data Privacy Act of 2012, the Philippines has not been spared from data breaches and violations relating to data protection, including those affecting government databases and involving sensitive personal information.[49] The unbridled rise of digital lending applications and the National Privacy Commission's inability to enforce its regulatory mandate resulted in thousands of privacy violations, including instances of harassment, which continued well into the pandemic period in 2020.[50] In late 2021, Filipino mobile subscribers were plagued by a spate of spam and phishing attacks, which in turn facilitated a number of bank fraud incidents and cast doubt on the effectiveness and reliability of regulators, banking institutions, and telecommunication service providers.[51]

[49] CNN Philippines. 'Data breach' reportedly exposes 345K sensitive SolGen documents. Available at https://www.cnnphilippines.com/news/2021/5/3/-Data-breach--reportedly-exposes-345K-sensitive-SolGen-documents-.html

[50] Foundation for Media Alternatives. Loan Apps: Financial inclusion at what cost? Available at https://www.fma.ph/wp-content/uploads/2021/02/FA-FMA-loan-apps-report-digital-share.pdf

[51] Philstar.com. House probe sought into scam texts and spam messages. Available at https://www.philstar.com/headlines/2021/12/06/2146126/house-probe-sought-scam-texts-and-spam-messages

IV. Recommendations

38. In light of the above issues, we call on the UN member states to make the following recommendations to the government of the Philippines:

On freedom of expression

- Review the Cybercrime Prevention Act of 2012 and its implementing rules and regulations and take immediate steps to repeal or amend the law in line with international human rights standards, including with respect to the right to freedom of expression.
- Repeal Section 4(c)4 of RA 10175 on online libel and likewise decriminalize libel in the country.
- Investigate all cases of threats, intimidation, and attacks against independent media personnel and human rights defenders and ensure that those responsible are held accountable
- Guarantee the establishment of a safe and enabling environment for the work of human rights defenders, specifically through the adoption of a law for the protection and recognition of human rights defenders
- Promote a safe and enabling environment for the work of human rights defenders, through the adoption of a charter for their protection and recognition.

On freedom of expression and sexual rights

- Repeal Section 4(c)1 of RA 10175 on cybersex and implement and strengthen existing laws that protect women against violence, sexual harassment, and abuse.

On online violence against women

- Protect women's rights online and take immediate and effective action to respond to all forms of online gender-based violence, including through the implementation of rights-compliant laws and non-legal initiatives, framed and implemented through public consultation with relevant stakeholders including civil society .[52]
- Develop policies on how ICTs can help promote women's empowerment and agency.
- Continue capacitating stakeholders to have a deeper understanding of how technology works and impacts women's rights. Support capacity-building for civil society organizations, especially women's organizations, including how to protect and secure their data online, as well as respond to cases of OGBV.

[52] A/HRC/RES/38/5. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/5

- Regularly engage with women's groups in aligning the development, adoption and implementation of policies and community standards with international human rights laws and women's rights commitments.
- Ensure that women, including those from the sectors of persons with disabilities, indigenous peoples, and LGBTQI, have representation and meaningful participation in policy discussions and decision-making.
- Ensure women's access to justice by having independent and effective redress mechanisms in place, including an enabling environment, not just legal, that is able to address women's issues on VAW, including ICT related VAW.
- Support capacity-building of judges, prosecutors, and law enforcers to ensure that Philippine laws protect and promote human rights in the face of rapidly changing technologies, while ensuring gender sensitivity in handling cases.
- Ensure that policies in schools are in place to respond to incidents of bullying offline and online and consider the inclusion in the school curricula of emerging issues such as cyber bullying and online gender-based violence.
- Continue to strengthen government policies to promote gender equality and eliminate all forms of discrimination and violence against women and children, including their safety both online and offline.

On privacy and data protection

- Take measures to ensure that provisions requiring for independent judicial authorization of communication surveillance are respected and implemented, and that in such cases, limitations on privacy are strictly and narrowly in compliance with the international legal principles of legality, necessity, and proportionality.
- Ensure that all government authorities permitted to undertake communications surveillance are subject to independent and effective oversight to ensure their operation in compliance with international human rights law, particularly with respect to protecting the rights to privacy, expression, and association.
- Review the Data Privacy Act of 2012 to establish a comprehensive legal framework for data protection with adequate and effective privacy safeguards; which will be implemented and overseen by an independent, impartial and adequately resourced data protection authority. The development of these legislations should be transparent and include public consultation with legal and technical experts in the field of data protection, members of civil society, academia, and the government, and seek coordination and advice from international data protection authorities and experts.
- Ensure that the National Privacy Commission enjoys full independence and authority and is adequately resourced in the conduct of its functions.
- Ensure that all existing and future laws, policies, and government systems are compliant with the provisions and consistent with the principles of the Data Privacy Act of 2012 and with international rights-focused best practices on data protection.

- In line with the above recommendation, repeal the Anti-Terrorism Act of 2020 or amend its provisions in line with international human rights law, in particular amending the expanding of the State's authority for communications surveillance.
- Conduct regular privacy audits (i.e., privacy impact assessments) on key, if not all, government agencies and offices.
- Provide redress for human rights violations concerning the right to privacy and data protection by strengthening the National Privacy Commission's grievance and accountability mechanisms.