COMMISSION ON HUMAN RIGHTS OF THE PHILIPPINES

INPUTS TO HUMAN RIGHTS COUNCIL ADOPTED RESOLUTION 34/7 ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE

9 April 2018

Introduction

1. The Commission on Human Rights of the Philippines (hereinafter the "Commission")[1] submits its written inputs to the Office of High Commissioner for Human Rights (OHCHR) as contribution to the report of the High Commissioner on the challenges relating to the right to privacy in the digital age, including principles, standards and best practices with regard to the promotion and protection of the right to privacy.

2. The inputs from the Commission took into consideration local and international reports from government, civil society, the media, and international non-government organizations. This submission also utilized the Commission's own documentation of independent monitoring activities and statements which were subjected to the internal deliberations of the Commission En Banc.

Legal Framework

1. The digital age,sometimes referred to as computer age or information age is now predominant due to the advancement in the use of digital technology. Currently, political, social and economic activities are being run by application of information and communication technologies (ICT).

---

[1] As the National Human Rights Institution (NHRI) of the Philippines, the Commission on Human Rights of has the mandate vested by the 1987 Philippine Constitution and the Paris Principles to promote and protect the full range of human rights including civil and political rights, and economic, social and cultural rights. It has the responsibility to regularly report and monitor human rights situations and violations, and recommend steps in advancing the realization of human rights and dignity of all. The Commission has "A"-status accreditation from the Sub-Committee for Accreditation of the Global Alliance of National Human Rights Institutions (GANHRI).

2. The internet was introduced to the Philippines in 1994 and since then, there has been a significant increase in the number of the people in the country using the internet. Current internet users are approximately 67 million and is now the world leader in terms of social media usage. [2]

3. With this progress, the following laws and policies were created to address technological advancement:

    - Republic Act No. 10173 Otherwise Known as Data Privacy Act of 2012- An Act Protecting Individual Personal Information In Information And Communications Systems In The Government And The Private Sector, Creating For This Purpose A National Privacy Commission, And For Other Purposes[3]
    - Republic Act No. 8972 Otherwise Known as E-Commerce Act of 2000 - An Act Providing For The Recognition And Use Of Electronic Commercial And Non-Commercial Transactions And Documents, Penalties For Unlawful Use Thereof, And For Other Purposes[4]
    - Republic Act No. 9775 Otherwise Known as Anti-Child Pornography Act of 2009 - An Act Defining The Crime Of Child Pornography, Prescribing Penalties Therefor And For Other Purposes[5]
    - Republic Act No. 9995 Otherwise Known as Anti-Photo and Video Voyeurism Act of 2009 - An Act Defining And Penalizing The Crime Of Photo And Video Voyeurism, Prescribing Penalties Therefor, And For Other Purposes[6]
    - Republic Act No. 10175 Otherwise Known as Cybercrime Prevention Act of 2012 - An Act Defining Cybercrime, Providing For The Prevention, Investigation, Suppression And The Imposition Of Penalties Therefor And For Other Purposes[7]
    - Republic Act No. 10364 Otherwise Known as Expanded Anti-Trafficking in Persons Act of 2012 - An Act Expanding Republic Act No. 9208, Entitled "An Act To Institute Policies To Eliminate Trafficking In Persons Especially Women And Children, Establishing The Necessary Institutional Mechanisms For The Protection And Support Of Trafficked Persons, Providing Penalties For Its Violations And For Other Purposes". [8]

4. Reliance on data-driven analytics, innovations, and decisions has a huge impact to the right to privacy of individuals. Undoubtedly, big data has its rewards but it also poses risks. Both Houses of the Philippine Congress are now proposing for the establishment of a Big Data Center in the Philippines that will develop a range of standards to use software and tools for analytics on massive amounts of data being generated from the use of the Internet and other technology. The proposals, which are pending for consideration in the

---

[2] Miguel R. Camus, *"Philippine is world leader in social media usage",* Published by Inquirer.net, Feb. 15, 2018, 5:24am http://business.inquirer.net/246015/ph-world-leader-social-media-usage, Last accessed: 28 March 2018.
[3] National Privacy Commission website, *"Republic Act 10173 – Data Privacy Act of 2012"*, https://privacy.gov.ph/data-privacy-act/, Last accessed: 28 March 2018.
[4] Republic Act No. 8972 Otherwise Known as E-Commerce Act of 2000
5 Republic Act No. 9775 Otherwise Known as Anti-Child Pornography Act of 2009
6 Republic Act No. 9995 Otherwise Known as Anti-Photo and Video Voyeurism Act of 2009
7 Republic Act No. 10175 Otherwise Known as Cybercrime Prevention Act of 2012
[8] Republic Act No. 10364 Otherwise Known as Expanded Anti-Trafficking in Persons Act of 2012

Committee level of both Houses, include provisions creating another layer of protection to the existing protective measures against data breaches that violates the right to privacy in the Data Privacy Act. The extent of the protective measures proposed have yet to be carefully studied.[9]

5. There is also a proposal to regulate Subscriber Identity Module (SIM) cards used in handheld phones in both Houses of Congress with the objective to help law enforcement agencies in tracking down lawless criminals who use mobile phones to pursue nefarious activities. The proposal in the lower house includes a Confidentiality Clause which prohibits disclosure of any information of a subscriber unless upon subpoena or lawful order from a competent court or written request from law enforcement agency in relation to an ongoing investigation, that a particular number requested is used in the commission of a crime. Whether this is sufficient to curtail possible breaches of the right to privacy is yet to be determined.[10]

Institutional Safeguards

6. In 2016, the Department of Information and Communications Technology (DICT) was established. DICT is mandated to be the primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national ICT development agenda (RA 10844). The DICT has the following powers and functions: [11]
    a. Policy and Planning
    b. Improved Public Access
    c. Resource-sharing and Capacity Building
    d. Consumer Protection and Industry Development
    e. Cybersecurity Policy and Program Coordination
    f. Countryside Development

7. Attached to the DICT is the National Privacy Commission (NPC) and the National Telecommunications Commission (NTC), which were also established in 2016. The National Privacy Commission is an independent body mandated to administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection. It acts as a country's privacy watchdog. [12]

---

[9] Senate Bill No. 688 and House Bill No. 3056 - An Act Institutionalizing the Establishment of the Philippine Big Data Center, Last accessed: 18 April 2018.

[10] Senate Bill No. 1219 - An Act Institutionalizing The Establishment Of The Philippine Big Data Center and House Bill No. 7233 – An Act Requiring the Registration of All Users of Subscriber Identity Module Card, Last accessed: 18 April 2018.

[11] Department of Information and Communication Technology official website, "*Mandate, Powers and Functions*", http://www.dict.gov.ph/about-us/our-mandate/, Last Accessed: 28 March 2018

[12] National Privacy Commission official website, https://privacy.gov.ph/about-us/#visionmission, Last Accessed: 28 March 2018.

6. The National Privacy Commission, as a Privacy Enforcement Authority (PEA) for the Philippines, joined the APEC Cross Border Privacy Enforcement Arrangement (CPEA), becoming the eleventh PEA along with those from eight other APEC economies namely, Australia, Canada, Hong Kong, Japan, Republic of Korea, New Zealand, US, and Mexico. The Philippines backstop enforcement network developed for the Cross-Border Privacy Rules (CBPR). These initiatives will promote effective cross-border privacy cooperation; it will also facilitate information sharing among privacy enforcement in APEC economies, and encourage information sharing and cooperation with authorities outside APEC.[13]

7. The National Telecommunications Commission (NTC) has the following mandates: [14]
    a. regulate the installation, operation and maintenance of radio stations both for private and public use (Act No. 3846, as amended);
    b. Regulate and supervise the provision of public telecommunications services (RA 7925, CA146 as amended);
    c. manage the radio spectrum (Act No. 3846, as amended and RA7925); and,
    d. Regulate and supervise radio and television broadcast stations, cable television (CATV) and pay television (EO546 and EO205).

Examples of privacy breach and issues on right to privacy

Data Privacy

1. In 2016, the website of the Commission on Elections (COMELEC) was hacked. Millions of voter registration records were exposed and this was considered the biggest leak of personal data in Philippine history.[15] The incident became the first case of the National Privacy Commission (NPC) and an eye opener for the government authorities to provide much-needed attention in securing personal data information.

2. Just this April, Facebook admitted that personal data of over 1.1 million Filipino Facebook users were improperly shared with a British political consulting firm, Cambridge Analytica. The National Privacy Commission has already launched an investigation to determine the extent of the data privacy breach, culpability of the parties involved, and the redress available.[16]

---

[13] National Privacy Commission website, "*PH Strengthens Extraterritorial Reach through the APEC Cross Border Privacy Enforcement Arrangement*", December 5, 2017, 11:55 am last edit December 7, 2017, https://privacy.gov.ph/ph-strengthens-extraterritorial-reach-apec-cross-border-privacy-enforcement-arrangement/, Last Accessed: 28 March 2018.

[14] National Telecommunication Office official website, http://ncr.ntc.gov.ph/?page_id=7, Last Accessed: 28 March 2018.

[15] Michael Bueza, "*Is Comelec liable for website data leak?*" Published by Rappler, April 11, 2016, 9:45am, https://www.rappler.com/newsbreak/in-depth/127465-comelec-hackers-liability-website-hacking-data-leak, Last Accessed: 28 March 2018.

[16] Natashya Gutierrez, *"Did Cambridge Analytica use Filipinos' Facebook data to help Duterte win?",* Published by Rappler, 6 April 2018, 5:02pm, https://www.rappler.com/nation/199599-facebook-data-scandal-cambridge-analytica-help-duterte-win-philippine-elections, Last Accessed: 06 April 2018.

3. A resolution at the House of Representatives was filed to investigate on the matter of a possible data breach of the Philippine Overseas Employment Administration (POEA). According to the House Resolution, data collected by the POEA, including sensitive information on the deployment of overseas Filipino workers, are stored in external servers held by its private company provider via a system of cloud computing, despite the lack of an existing contract with the private company. The House of Representatives Committee on Overseas Workers Affairs has yet initiated the investigation on the matter.[17]

Digital surveillance

4. Former Secretary of the Department of Justice, Senator Leila De Lima is currently detained at the PNP custodial center due to her supposed involvement in the illegal drug trade. Her phone conversation with her driver was used against her as evidence. [18] In 2016, a bill seeking to amend the anti-wiretapping law has been approved at the committee level. The bill seeks to allow wiretapping on highway robbery, coup d'état and drug cases. [19]

5. In 2005, the Philippine former president Gloria Macapagal Arroyo was involved in a controversial "Hello Garci" scandal. Her conversation with Comelec Commissioner Virgilio Garcilliano has been wiretapped. The House and Senate conducted investigations and netizens made a call for the resignation of the president. [20]

6. Karapatan, an NGO working for the promotion and protection of human rights in the Philippines reported physical surveillance. According to Ms. Cristina Palabay, Karapatan's Secretary General, they have to cancel several meetings because they knew somebody is tailing and watching over them. They also discovered a tracking device in one of their service vehicles after they got it back from custody at the Manila Police District during the Association of Southeast Asian Nations (ASEAN) Summit in November 2017. On the other hand, Amnesty International Philippines Chairperson Ritz Lee Santos stated that there were instances that she is receiving alerts that someone is trying to hack her account and email address. [21]

7. The Philippine government also tag at least 600 individuals as a terrorist in a list of supposed leaders and members of the Communist Party of the Philippines (CPP) and the

---

[17] House Resolution No. 1749, Last Accessed: 18 April 2018.

[18] Mark Merueñas, "*De Lima maintains innocence despite Duterte's alleged wiretap, ATM evidence",* Published by GMA News Online, August 23, 2016, 5:51pm, http://www.gmanetwork.com/news/news/nation/578670/de-lima-maintains-innocence-despite-duterte-s-alleged-wiretap-atm-evidence/story/, Last Accessed: 28 March 2018.

[19] Maila Ager, "*Bill seeking wiretaps in drug cases moves up in Senate*", Published by Inquirer.net, October 20, 2016, 11:51am, http://newsinfo.inquirer.net/827919/bill-seeking-wiretaps-in-drug-cases-moves-up-in-senate, Last Accessed: 28 March 2018.

[20] "*Hello Garci scandal*", Published by GMA News Online, January 25, 2008, 6:29pm, http://www.gmanetwork.com/news/news/content/27477/hello-garci-scandal/story/, Last Accessed: 28 March 2018.

[21] Jodesz Gavilan And Sofia Tomacruz, *"PRONE TO ABUSE State surveillance as a tool to silence critics",* Published by Rappler, April 2, 2018, 6:09pm, https://www.rappler.com/newsbreak/in-depth/198128-philippines-government-surveillance-abuse-human-rights-violation-silence-critics, Last Accessed: 4 April 2018

New People's Army (NPA). The list includes several human rights defenders and individual activist who continuously criticized the current government. [22]

Effects of undue interferences with the right to privacy in the digital age to the following:

Women[23]

1. In the digital age where majority of the citizens have access to the internet and other information and communications technology, people, especially women, are exposed to greater risks of online harassment and violence. Following a mapping of online gender-based violence in the Philippines conducted by the Foundation for Media Alternatives (FMA), it was found that there have been more than one hundred and sixty (160) cases of online gender based violence cases in the country since 2012. These include incidents of online harassment, cyber bullying, digital stalking, identity theft, verbal sexual assault, threats and abusive comments, and uploading of photos and videos on intimate nature without consent.

2. One example would be the case of human rights defender and climate advocate Renee Juliene Karunungan, who was prompted to file an election offense case against 20 supporters of then Davao City mayor and candidate for President Rodrigo Duterte before the Commission on Elections after she received threats of rape, physical violence, and harassment last May of 2016. Karunungan was subjected to such threats both online and offline after she spoke up against Duterte's candidacy.

3. Another notable incident of online harassment was against a woman whose photo circulated online following a protest against the burial of late President Ferdinand Marcos. The protestor's photo was feasted on by male netizens with comments containing vulgar descriptions, including sexual harassment and rape threats.

4. In response to the increasing incidence of sexual harassment, misogynist attack and unwanted remarks against women both online and offline, in 2016, Senator Risa Hontiveros filed three bills dubbed as the 'Tres Marias bills' which are The Anti-Rape Act, Anti-Sexual Harassment Bill, and the Gender-Based Electronic Violence Bill. The said measures seek to strengthen the existing Anti-Rape Law, criminalize peer-to-peer sexual harassment and impose penalties on perpetrators of misogynistic and homophobic attacks on social media and other multimedia sites.

5. The Gender-Based Electronic Act (Senate Bill No. 1251) seeks to prohibit and impose penalties on people behind misogynistic and homophobic attacks on social media, which it brands as gender-based electronic violence. According to Senator Risa Hontiveros, many of the victims of gender-based electronic violence are young people, who use social media as their primary outlet of expression. These attacks have the effect of silencing this

[22] *Idem*

[23] CHR Inputs on HRC 32/13 on the The Promotion, Protection And Enjoyment Of Human Rights On The Internet, 29 January 2017

expression, and contributing to a culture of misogyny and hate. In sum, the bill proposes to institute protective measures such as the issuance of a protective order, the imposition of penalties against perpetrators and the provision of educational tools against gender-based electronic violence. The bill affords protection not only to women and girls but also to persons with diverse SOGIE.

6. In August 2017, The Anti-Sexual Harassment Bill proposed by Senator Hontiveros, (Senate Bill No. 1250) has been substituted by Senate Bill No. 1558, otherwise known as the 'Safe Streets, Workplaces and Public Spaces Act of 2017'. The said bill has the effect of amending the Anti Sexual Harassment Act of 1995, expanding the definition of Sexual Harassment in the Workplace as to include 'acts involving unwelcome sexual advances, requests or demand for sexual favors or any act of sexual nature, whether done verbally, physically or through the use of technology such as text messaging or electronic mail or communication that has or could have a detrimental effect on the conditions of an individual's employment or education, job performance or opportunities.'

7. In addition to the said pending bills, Senator Nancy S. Binay likewise introduced Senate Bill 180 'An Act Amending Republic Act No. 9262, Defining the Electronic Violence Against Women or E-Vaw, Providing Protective Measures and Prescribing Penalties Therefor, and for Other Purposes'. The said bill seeks to amend the VAWC Law to include electronic violence against women and to offer protection to women in the form of E-VAW Protection Orders. The bill likewise sets out penalties for acts of violence against women committed through electronic means.

8. To date, there are still no existing legislations catering specifically to online violence against women as the proposed bills mentioned are still under deliberation in the Congress. However, victims of online harassment may seek redress under Republic Act No. 10175, or the Cybercrime Prevention Act, the Civil Code on Damages (Art. 2176) or under The Labour Code on Just Causes for Termination (Sec. 5.2(g), D.O 147-15). The mentioned acts are, however, focused only on any act similar to cyberlibel, slander, intriguing against honour and prying into the privacy of another and does not directly cater to women.

9. The Department of Justice (DOJ) Cybercrime Division Group enumerated procedures on how one can seek redress against online harassment:
    a. Victims of online harassment cases may report through the DOJ Cybercrime Division, the National Bureau of Investigation Cybercrime Division and the Philippine National Police Cybercrime Group which accepts and handles cases of such nature.
    b. The reporting must be done personally by the victims.
    c. When filing a report, it is necessary to present proof of cyberbullying and harassment such as screenshots and other "receipts"
    d. Once equipped with evidence, the victim will be asked to furnish a formal complaint by submitting an affidavit narrating the crime or offense imputed.

10. Under Republic Act No. 10175, or the Cybercrime Prevention Act, any person found guilty of committing the unlawful or prohibited acts of libel, as defined in Article 355 of the

Revised Penal Code , may be punished with prision correccional in its maximum period to prision mayor in its minimum period or a fine ranging from P6,000.00 up to the maximum amount determined by the court. The provision however only applies to the original author of the post of online libel and not to others who simply received the post and or who just react to it or shared it.

Existing policies that allow identification, reporting and rectification of incidents of harassment or violence against women via the internet services providers:

11. Under the Implementing Rules and Regulations (IRR)of Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012", "law enforcement authorities, upon issuance of a court warrant, shall be authorized to collect or record by technical or electronic means, and the service providers are required to collect or record by technical or electronic means and/or to cooperate and assist in the collection or recording of computer data that are associated with specified communications transmitted by means of a computer system" (Sec. 13, IRR).

12. The IRR likewise provides power to the DOJ to issue preservation orders addressed to service providers and to monitor compliance of the service providers with regard to the duties imposed upon them under Rule 7 of the IRR as follows:

    a. Preserve the integrity of traffic data and subscriber information for a minimum period of six (6) months from the date of the transaction;

    b. Preserve the integrity of content data for six (6) months from the date of receipt of the order from law enforcement or competent authorities requiring its preservation;

    c. Preserve the integrity of computer data for an extended period of six (6) months from the date of receipt of the order from law enforcement or competent authorities requiring extension on its preservation;

    d. Preserve the integrity of computer data until the final termination of the case and/or as ordered by the Court, as the case may be, upon receipt of a copy of the transmittal document to the Office of the Prosecutor;

    e. Ensure the confidentiality of the preservation orders and its compliance;

    f. Collect or record by technical or electronic means, and/or cooperate and assist law enforcement or competent authorities in the collection or recording of computer data that are associated with specified communications transmitted by means of a computer system, in relation to Section 13 hereof;

    g. Disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control to law enforcement or competent authorities within seventy-two (72) hours after receipt of order and/or copy of the court warrant;

    h. Report to the DOJ – Office of Cybercrime compliance with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof;

i. Immediately and completely destroy the computer data subject of a preservation and examination after the expiration of the period provided in Sections 13 and 15 of the Act; and

j. Perform such other duties as may be necessary and proper to carry into effect the provisions of the Act.

Existing jurisprudence from international, regional, and national courts, on prosecution or administrative proceedings in such cases;

13. Due to the absence of concrete legislative enactment directly for the apprehension of online violence and sexual harassment against women in the Philippines, there are still no existing jurisprudence available on the subject matter. However, there are decided cases by the Supreme Court concerning violations of the Anti-Violence Against Women and Their Children (Republic Act No. 9262) through the use of electronic devices, one of which is the case of Pascua vs. CA as discussed below:

14. In the case of Rustan Ang y Pascua vs. The Honoroable Court of Appeals and Irish Sagud decided by the Supreme Court in 2010, the accused willfully and unlawfully sent through SMS using his mobile phone, a pornographic picture to one Iris Sagud, who was his former girlfriend whereby the face of the latter was attached to a completely naked body of another woman making it to appear that it was said Irish Sagud who is depicted in the said obscene pictures thereby causing substantial emotional anguish, psychological distress and humiliation to the victim. The Supreme Court decided in favor of the respondent, finding the accused guilty of the violation of Section 5(h) of Republic Act No. 9262 or the Anti-Violence Against Women and Their Children Act.
http://sc.judiciary.gov.ph/jurisprudence/2010/april2010/182835.htm

15. The Commission on Human Rights, as Gender Ombud[24] currently has limited capacity to investigate online VAW or Sexual Harassment cases. Nonetheless, the Commission recommends cases of this nature to the Department of Justice (DOJ) specifically to National Bureau of Investigation and the Anti- Cybercrime Group. The Commission likewise has the power to monitor the concerned government agencies responsible for the resolution of cases of online violence; as such, the Commission has the mandate to call out such agencies in case of inadequacy in providing protection for women facing cases of online violence.

Children

16. Based on the data that was reported by the UNICEF, around 80% of the Filipino children are at risk of online sexual abuse and the Philippines is considered as top global source of child pornography.[25] Despite the conduct of police raids, arrests made and cases filed the courts, cybersex operations that involve children are still very common. In some cases,

---

[25] Patty Passion, "*Philippines top global source of child pornography – Unicef*", Published by Rappler, December 13, 2017, 11:58pm, https://www.rappler.com/nation/191219-philippines-top-global-source-child-pornography-unicef, Last Accessed: 28 March 2018.

children are molested by pornography operators, or are otherwise being forced to expose themselves on camera to have sex with each other. [26]

17. In a report submitted by the Foundation for Media Alternatives as contribution to the Universal Periodic Review of the Philippines last May 2017, the Inter-Agency Council Against Child Pornography (IACACP) presented the following at the ITU-ASEAN Workshop on Child Online Protection held in September 2016:[27]
    a. From January to September 2015, it handled 129 cases and requested 314 websites for blocking;
    b. The Philippine Center for Transnational Crime (PCTC), a member of the IACACP, received 71 cases from Interpol involving child pornography; and,
    c. The Department of Social Welfare and Development (DSWD) received a total of 121 reports of child pornography cases in 2014.

18. Aside from Republic Act No. 9775 Otherwise Known as Anti-Child Pornography Act of 2009, the Philippine government, as part of its initiative to protect children's welfare online, included a child online protection provision in Republic Act 10929 also known as the Free Internet in Public Places Act.[28]

CHRP initiatives[29]

Wiretapping

- In a 1997 position paper on House Resolution No. 1347, the CHRP condemned the illegal wiretapping practices of state-funded intelligence agencies and recommended: (1) to amend the Anti-Wiretapping Act to make it more responsive and attuned to present realities; and (2) for intelligence agencies to establish a mechanism to ensure their compliance with the law and to ensure accountability in the event of breach of individual rights.
- In a 1999 position paper, the CHRP expressed strong support for the immediate enactment of Senate Bill No. 680, "An Act Prohibiting Wire, Electronic, and Oral Communications Interception and Providing Penalties Therefor," and maintained that electronic eavesdropping is an infringement of an individual's right to privacy of communication enshrined in Article 12 of UDHR, Article 17 of ICCPR, and Article 3 Section 3 of the Constitution.

---

[26] "*Human Rights And The Philippine Digital Environment*", Joint Submission To The Universal Periodic Review of The Philippines (for consideration at the 27th session of the Working Group in April-May 2017), Published by FMA, September 2016, https://www.upr-info.org/sites/default/files/document/philippines/session_27_-_may_2017/js11_upr27_phl_e_main.pdf, Last Accessed: 28 March 2018.

[27] *Idem*

[28] *Idem*

[29] CHR's presentation during the stocktaking meeting with National Privacy Commission and Forum for Media Alternatives, 9 May 2017.

National & Barangay ID System

- In July 2006, the CHRP released a comment in support of the call for a national ID system taking into consideration its material benefits and the assurance of compliance with human rights standards that safeguard the individual's right to privacy.

- In February 2008, CHRP Region IX, Zamboanga released a legal opinion on the implementation of an ID system in Patikul, Sulu, strongly opposing such policy for being unconstitutional on the ground that it violates the people's right to privacy and freedom of movement.

- In January 2018, the CHRP release its Position Paper on the Proposal to Establish a National ID System. [30]

> "The CHR recognizes the material benefits of establishing a national ID system and supports the national government in aiming for policies that promote the right of persons to access social services. Furthermore, the CHR acknowledges that developments in the present legal framework of the country by providing more safeguards in protecting an individual's right to privacy with the enactment of Republic Act No. (RA) 10173, or the Data Privacy Act of 2012, and in the technological capacities of the government to handle robust databases, create a more conducive environment for a national ID system to achieve its objectives while protecting the rights of individuals. The CHR also notes that the proposed legislative measures provide in the collection, recording, and accessing of individual information entered in the proposed system. The bills provide protection against unlawful disclosure of information/records, penal sanctions, clear institutional responsibilities, and safeguard against derogation of rights or denial of services by failure to present an ID card. Given the foregoing, the CHR supports the establishment of a national ID system that complies with international human rights obligations and standards herein discussed. The bills pending in the 17th Congress proposing the establishment of such a system must be subjected to thorough review to ensure compliance with human rights obligations and standards".

Freedom of Information

- In a 2009 position paper on the FOI Bill, the CHR recommended that under an FOI framework, there should be a balance of what can and cannot be made public taking into consideration all factors that will best promote, protect and respect the human rights of as many stakeholders possible.

---

[30] CHR's Position Paper on the Proposal to Establish a National ID System, 15 January 2018.

- The Commission noted the exemptions provided under the Act. However, the Commission recommended to give attention to confidential information of vulnerable sectors of the society, such as women and children who may have been subjects of abuse, trafficking and similar forms of violence, to information with respect to the rehabilitation of people under the influence of drug abuse and to other information which maybe best left private even if part of public records. This may constitute an infringement of their right to privacy.

- While the Commission noted and concurred with the procedure and guidelines set forth under Section 9 to 15 of this bill for seeking information as properly laid out, the Commission recommended to provide additional exemption for its application in matters of extreme urgency involving human rights. By this, the Commission meant information involving the whereabouts of persons believed to be victims of enforced disappearance, extrajudicial killings, torture and other human rights violations. In these instances, following strictly the procedures herein provided may mean loss of precious time needed to prevent further damage and prejudice to victims. Proper government agencies must not be given a justification, in the guise of this law, to conceal information relevant to any investigation for violations of human rights.

Radio Frequency Identification

- In a 2009 advisory on RFID technology in vehicle registration and identification, thoroughly discussed the human rights standards that such technology should adhere to, and recommended the following:
    1. For the LTO to conduct the necessary consultations and dialogues on such technology and its implications;
    2. For the LTO to craft the necessary guidelines for the application of the RFID technology taking into consideration all HR standards;
    3. For Congress to look into the possibility of enacting a law elaborating on the right to privacy and the proper handling of personal information by responsible government agencies.