PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
27th Session – Philippines

The Right to Privacy in the Philippines

Submitted by the Foundation for Media Alternatives and Privacy International

September 2016

PRIVACY INTERNATIONAL

Foundation for Media Alternatives

Introduction

1. Pursuant to Human Rights Council (HRC) Resolution 5/1, Privacy International (PI) and the Foundation for Media Alternatives (FMA) present this submission as non-governmental organizations (NGOs) to supplement the report of the Government of the Philippines (the Government), scheduled for review by the HRC during its 27th session.

2. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance and promote the right to privacy and fight surveillance around the world. FMA is a Philippine-based NGO that assists individuals and communities in their strategic and appropriate use of information and communications media for democratization and popular empowerment.

3. This submission presents information about recent developments and ongoing human rights violations that relate to the right to privacy in the Philippines as a result of persistent legal, policy, and practical barriers to a comprehensive and rights-based privacy framework.

The right to privacy

4. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

5. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2]

6. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to

1 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.

2 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.

the protection of personal data.[3] A number of international instruments enshrine data protection principles,[4] and many domestic legislatures have incorporated such principles into national law.[5]

Domestic laws related to privacy

7. According to the Philippine Constitution, one of the fundamental policies of the State is to put premium on the dignity of every person and guaranteeing full respect for their human rights.[6]

8. The 1987 Constitution of the Philippines protects against unreasonable searches and seizures,[7] and renders inviolable the privacy of their communication and correspondence[8]:

> "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 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."

International obligations

9. The country also adopts generally accepted principles of international law as part of the law of the land.[9] Accordingly, it is duty-bound to observe the right to privacy, as enshrined in such international legal instruments as the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights (ICCPR). The Philippines has ratified the ICCPR.

Follow up to the previous UPR

10. The previous UPR (both the National Report and the report of the Working Group) made no mention of the right to privacy, nor of any privacy-related violations in the Philippines. However, privacy issues in the Philippines have become significantly more prominent since the last UPR cycle.

3 Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17)See: A/HRC/WG.6/13/MAR/3, para. 37

4 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

5 As of December 2013, 101 countries had enacted data protection legislation.
See: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

6 1987 Constitution, Article II, §11.

7 Ibid, Article III, §2.

8 Ibid, §3.

9 1987 Constitution, Article II, §2.

Areas of concern

I. Communications Surveillance

11. In May 2016, Rodrigo Duarte was elected as the President of the of the Philippines. Since his election, President Duarte has presented his position on various policies (including on the war of drugs[10]). These policies in addition to the lack of oversight of state surveillance and the increase in the capacity of police and other agencies to conduct intrusive surveillance, pose a significant risk that unlawful surveillance will result not only the violation of individuals' privacy but also in enabling other serious human rights violations.

12. It is urgent that President Duarte takes various measures to ensure that authorities permitted to undertake surveillance are regulated by a robust legal framework that upholds principles of legitimacy, proportionality and necessity to ensure that any interference with privacy is targeted and not arbitrary, as well as legislate for prior judicial authorisation, independent oversight, user notification, and access to remedy in case of violations.

Interception of communications

13. In the Philippines, there are various laws which regulate communications surveillance, these include Anti-Wiretapping Law of 1965 (Republic Act No. 4200), the Anti-Photo and Video Voyeurism Act of 2009 (Republic Act No. 9995), the Cybercrime Prevention Act of 2012 (Republic Act No. 10175) and the Human Security Act of 2007 (Republic Act No. 9372)[11]

14. While the Philippine legislation prohibits unauthorised wiretapping and other violations of the privacy of communication,[12] it allows lawful interception when such activity is authorized by a written court order in relation to cases involving specific crimes (e.g., treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, sedition, and kidnapping)[13].

15. Particularly following the election of President Duterte, a range of bills have been tabled to expand the crimes for which wiretapping can be authorised to cover the surveillance of a person, if there is probable cause tending to prove that the person has committed the crime of coup d'etat,[14] plunder and other graft and corruption offenses,[15] or has violated the Comprehensive Dangerous Drugs Act of 2002 (CDDA).[16]

10 See: Gutierrez, J., Body Count Rises as Philippine President Wages War on Drugs, The New York Times, 2 August 2016. Availble at: http://www.nytimes.com/2016/08/03/world/asia/philippines-duterte-drug-killing.html?_r=0

11 Other laws that impact the right to privacy include: the Expanded Anti-Trafficking in Persons Act of 2012 (Republic Act No. 10364)

12 Republic Act No. 4200, §1.

13 Id., §3.

14 See: Senate Bill No. 48, as filed by Senator Panfilo Lacson.

15 See: Senate Bill No. 339, as filed by Senator Grace Poe.

16 See: Senate Bill No. 2 submitted by Senator Gregorio Honasan II, House Bills No. 528, 3906, 5491, 5839, and 6107.and House Bills No. 289, 587, 1868, and 3406.

No implementation of oversight and accountability mechanism for the police

16. The Human Security Act provides for the establishment of a Grievance Committee to be composed of composed of the Ombudsman, the Solicitor General, and the undersecretary of the Department of Justice. Three sub-committees headed by the Deputy Ombudsmen in Luzon, the Visayas and Mindanao will assist the Grievance Committee to receive, evaluate and investigate complaints against the actuations of the police and law enforcement officials in the implementation of the Act. If the investigation results in the gathering of evidence, the sub-committees may file the appropriate cases against the concerned police and law enforcement officers. But this Committee has yet to be established.[17]

17. A Joint Oversight Committee, also provided for in the law, is to be composed of senators and members of congress. It has the power to summon members of the police and law enforcement authorities and the members of the Anti-Terrorism Council to be questioned regarding how they undertake surveillance of individuals. It also receives reports of the relevant agencies on their operations. The Joint Oversight Committee must present bi-annual reports to the Houses of Congress.[18] However such reports have not yet been published.[19]

18. It is essential that these two oversight mechanisms be fully implemented. An independent oversight mechanism is necessary to ensure the transparency and accountability of the surveillance authorisation processes. The oversight mechanism must be independent of the executive, properly resourced to conduct investigations, and able to command public confidence through regular reporting and public sessions.

No oversight of intelligence agencies

19. The Philippines has several intelligence agencies in place. These include The National Security Council (NSC), the Office of the National Security Adviser (ONSA), the National Intelligence Coordinating Agency (NICA), the National Intelligence Committee (NIC), the National Intelligence Board (NIB), the Intelligence Service, Armed Forces of the Philippines (ISAFP).

20. Concerns have been raised by the lack of transparency and oversight of these agencies.[20] There are no oversight mechanisms in place to oversee the mandate and the activities of these agencies and the President is the highest authority in matters of national security and most of the agencies

17 Caraig, J., The Human Security Act Of 2007 of the Philippines: Assessing the Law's Compliance with International Human Rights while Countering Terrorism, University of Oslo, Faculty of Law, 18 May 2010. Available at: https://www.duo.uio.no/bitstream/handle/10852/22869/joannaca_duo.pdf?sequence=1, pp. CC-DD

18 Ibid, pp. EE-FF

19 Bahague, R., Communications surveillance in the Philippines: Laws and the struggle for the right to privacy, in 'Global Information Society Watch 2014: Communications surveillance in the digital age', published by Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos). Available at: https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf, pp. 196

20 Domingo, F., Philippine Intelligence Community: A Case for Transparency, in 'Security Sector Reform: Modern Defense Force' published by Ateneo de Manila University (ADMU), Department of Political Science, 2014. Available at: http://www.academia.edu/6704814/Philippine_Intelligence_Community_A_Case_for_Transparency

report directly to him. The President chairs the National Security Council. The Council advises the President on the integration of domestic, foreign, military, political, economic, social and educational policies relating to national security.[21]

21. Policies on national security are the mandate of the National Intelligence Coordinating Agency (NICA) which is the main intelligence agency of the Philippine government. Since 1987, the mandate of NICA has expanded from "organize and coordinate the intelligence collection activities of various government instrumentalities concerned" to "directing, coordinating, and integrating all government activities involving national intelligence."[22]

22. In the two previous Congresses, several bills proposing oversight of the intelligence agencies were proposed, but never adopted.[23]

23. Independent oversight of intelligence agencies is fundamental to guarantee respect of human rights, including the right to privacy and freedom of expression. The mandate, remit and operations of all intelligence agencies must be reviewed to meet international standards. The State should be transparent about the use and scope of communications surveillance techniques and powers.

Regulations of Cybercrime Prevention Act

24. Section 12 (Real-Time Collection of Traffic Data) of the Cybercrime Prevention Act was stricken down as unconstitutional by the Supreme Court in the landmark case Disini v. The Secretary of Justice.[24] The provision would have authorized the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) to collect or record in real-time, with due cause, traffic data associated with specified communications transmitted by means of a computer system. The Supreme Court ruled that the provision threatens the Constitutional right to privacy, by giving law enforcement authorities sweeping and unrestrained authority. It held that "the grant of the power to track cyberspace communications in real time and determine their sources and destinations must be narrowly drawn to preclude abuses".

25. However, the Implementing Rules and Regulations (IRR) of the law, which were promulgated in August 2015, effectively reinstated the struck down provision. The Regulations broadly authorize law enforcement authorities, upon the issuance of a court warrant, "to collect or record by technical

21 Sec. 5(1), Chapter 2, Subtitle I, Title VIII, Book IV, Executive Order No. 292 (1987)
22 Domingo, F., Philippine Intelligence Community: A Case for Transparency, pp. 80, in 'Security Sector Reform: Modern Defense Force' published by Ateneo de Manila University (ADMU), Department of Political Science, 2014. Available at: http://www.academia.edu/6704814/Philippine_Intelligence_Community_A_Case_for_Transparency
23 In 2010, Jinggoy Ejercito Estrada introduced Senate Bill No. 765 ('Intelligence Oversight Act of 2010'), which never passed the Committee level. In the same year his half-brother Joseph Victor Ejercito filed the same proposal at the House of Representatives, but it also did not pass. In the succeeding Congress, Ejercito Estrada again introduced the bill at the Senate but it was never adopted. Availble at: http://www.senate.gov.ph/lis/bill_res.aspx?congress=16&q=SBN-783
24 Disini v. Secretary of Justice, GR No. 203335 (S.C., Feb. 18, 2014) (Phil.), Available at: http://sc.judiciary.gov.ph/jurisprudence/2014/february2014/203335.pdf

or electronic means [...] computer data that are associated with specified communications transmitted by means of a computer system."[25] The Rules effectively amend the Anti-Wiretapping Law by expanding anew the list of crimes exempted from the prohibition on communication surveillance to include all types of cybercrimes. Rules having the effect of amending a law and expanding the powers of surveillance is clearly unconstitutional and in violation of the principle of legality under international human rights law.

Data retention

26. The regime of data retention is outlined in the Implementing Rules and Regulations of the Electronic Commerce Act (2000). The act is intended to provide for the "recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes".[26] Section 20 of its Implementing Rules and Regulations[27] outlines appropriate forms of data retention and the mandate of "relevant government agencies" to impose regulations on data retention.

27. As part of its regulatory function, the National Telecommunications Commission released a memorandum (MC 04-06-2007)[28] in June 2007 on the data log retention of telecommunications traffic.[29] Section 1 states:

> "PTEs [public telecommunications entities] shall retain the call data records on voice calls and similar records for non-voice traffic. on-voice traffic includes SMS, MMS and other similar telecommunications services."

28. Section 2 states:

> "Records indicating traffic data on the origin, destination, date, time, and duration of communications shall be retained within the following periods:
> two (2) months for non-metered services with fixed monthly charges;
> four (4) months for other telecommunications services not covered in (a); or
> until excused by NTC for records requested in connection with pending complaints."

29. This provision effectively requires companies to indiscriminately retain personal data of all customers, which, as such, constitutes an unalwful interference with the right to privacy.[30]

25 Implementing Rules and Regulations of Republic Act No. 10175, §13.
26 See: http://icto.dost.gov.ph/wp-content/uploads/2014/10/images_ipenforcement_RA8792-E-Commerce_Act.pdf
27 Available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=225364
28 Available at: http://janette.digitalfilipino.com/wp-content/uploads/2015/03/MC-04-06-2007-DATA-LOG-RETENTION-OF-TELECOMMUNICATIONS-TRAFFIC.pdf
29 Bahague, R., Communications surveillance in the Philippines: Laws and the struggle for the right to privacy, in 'Global Information Society Watch 2014: Communications surveillance in the digital age', published by Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos). Available at: https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf, pp. 196
30 In Digital Rights Ireland v Minister for Communications and Others, the Grand Chamber of the Court of Justice of the European Union (CJEU) concluded that the 2006 Data Retention Directive, which required communications service providers to retain customer data for up to two years for the purpose of preventing and detecting serious crime, breached the rights to privacy and data protection. The CJEU observed that the scope of the data retention "entails an interference with the fundamental rights of practically the entire European population". The CJEU went on to note the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security, and concluded that the Directive amounted to a "wide-ranging and particularly serious interference" with the rights to privacy and data protection "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary". Full judgment available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Bills seeking to establish a mandatory SIM card registration system

30. Except for contracted subscribers of telecommunication companies, there is currently no mandatory requirement to have SIM cards registered. There have been efforts, however, to establish a mandatory SIM card registration scheme.

31. During the 16th Congress, the House of Representatives successfully passed House Bill No. 523 ("Subscriber Identity Module (SIM) Card Registration Act") which would require each SIM card end-user to verify his/her identity at the point of sale by presenting proof of identity. The bill did not see any development before the previous Congress adjourned. However, various bills proposing a similar policy have again been filed in the current Congress, accompanied by calls to have the same certified as an urgent measure in light of the supposed increase in the number of hoax bomb threats.[31]

Surveillance capabilities

32. Absent any public avowal by the authorities of their surveillance powers, evidence of the surveillance capabilities of the government has emerged primarily from the media and investigative journalists.

33. Over the years, several sources have hinted that the State has acquired or at least expressed interest in acquiring various interception tools, which would provide law enforcement and intelligence agencies in the Philippines with significant capacity to conduct intrusive surveillance, including social media monitoring, and remote hacking of devices.[32]

34. Since the election of current Philippine President Rodrigo Duterte, the government has been focused on its crackdown on the illegal drugs trade and surveillance is at the core of this work which means that is has become a key recipient of State resources.

35. If the 2017 budget proposal is approved, the Office of the President will get PhP2 billion in confidential and intelligence funds, up from PhP250 million this year[33], and PhP5.5 billion as contingency funds. When one opposition

31 Torregoza, H., Duterte urged to push SIM card registration, Manila Bulletin, 12 September 2016. Available at: http://www.mb.com.ph/duterte-urged-to-push-sim-card-registration/

32 These surveillance technologies include the following: Spectre, see: Wires, T., P135-M spy gadgets trained on opponents, The Daily Tribune. Available at: http://www.tribune.net.ph/headlines/p135-m-spy-gadgets-trained-on-opponents; Personal Identification Secure Comparison and Evaluation System (P.I.S.C.E.S.), see: U.S. Department of State, Office of Counterterrorism. Fact Sheet (2002). Available at: http://2001-2009.state.gov/s/ct/rls/fs/2002/12676.htm, Araneta, S., BI-NAIA to create anti-terror task force, The Philippine Star, 15 August 2004, Available at: http://www.philstar.com/metro/261297/bi-naia-create-anti-terror-task-force and Waterman, S., Americans placed on Filipino Watch List, International Labor Rights Forum, 12 October 2007. Available at: http://www.laborrights.org/in-the-news/americans-placed-filipino-watch-list; Signal, see: Intergen, Signal. Available at: http://www.intergen.co.nz/What-We-Do/Technology/Signal/ ; Galileo Remote Control System, see: Cruz, R., Duterte seeks billions in confidential, intel funds in 2017, ABS CBN News, 22 August 2016. Available at: http://news.abs-cbn.com/business/08/22/16/duterte-seeks-billions-in-confidential-intel-funds-in-2017, Salaveirra, L., Duterte defends Palace budget, Inquirer.Net, 26 August 2016. Available at: http://newsinfo.inquirer.net/809939/duterte-defends-palace-budget

33 Cruz, R., Duterte seeks billions in confidential, intel funds in 2017, ABS CBN News, 22 August 2016. Available at: http://news.abs-cbn.com/business/08/22/16/duterte-seeks-billions-in-confidential-intel-funds-in-2017

lawmaker questioned the significant increase, the President defended the budget by claiming that it would be used for his "many fights," as well as on "efforts to gather necessary intelligence data for government programs."[34] These assertions have been echoed by Budget Secretary Benjamin Diokno who said that the President's confidential and intelligence funds will be used in the fight against drugs and criminality.[35]

Lack of investigations of reports of Foreign Surveillance Activities

36. Documents released by Edward Snowden in May 2014 show that the US' National Security Agency (NSA) had "access via DSD asset in a Philippine provider site. Collects Philippine GSM, short message service (SMS) and Call Detail Records." This, the NSA predicted "[w]ill soon become a source of lucrative intelligence for terrorist activities in Southern Philippines."[36] The 2013 project. codenamed MYSTIC, involved the interception of large amounts of the communications of five countries, including the Philippines, from undersea cables.[37]

37. Such spying programmes by foreign governments directly threaten the privacy of Filipino citizens as well as the security of the telecommunication network and infrastructure. There is a need for an independent inquiry into the evidence provided which would also identify what measures must be taken to ensure that the Filipino government meets its international legal obligations to protect the right to privacy from external unlawful interference.

II. Data Protection

38. Although the Data Privacy Act was enacted in 2012, the National Privacy Commission, which is the agency tasked to administer and implement the law, was appointed only in March 2016.[38] Thus, prior to 2016, there was no government mechanism in place to monitor and protect data privacy.

39. Government agencies that collect and process personal data remained unregulated because they are exempt from the scope of application of the Act, which means that the storage and processing of large amounts of personal data collected by public bodies are subject to weak security measures against data breaches. This, in turn, made possible several data breaches over the years, the most prominent of which is the breach of the Commission on Elections's (COMELEC) voter database.

34 Salaveirra, L., Duterte defends Palace budget, Inquirer.Net, 26 August 2016. Available at: http://newsinfo.inquirer.net/809939/duterte-defends-palace-budget

35 Cruz, R., Duterte seeks billions in confidential, intel funds in 2017, ABS CBN News, 22 August 2016. Available at: http://news.abs-cbn.com/business/08/22/16/duterte-seeks-billions-in-confidential-intel-funds-in-2017

36 Devereaux, R., Greenwald, G., and Poitras, L., Data Pirates of the Caribbean: the NSA Is Reocrding Every Cell Phone Call in the Bahamas, The Intercept, 19 May 2014. Available at: https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

37 Diola, C., Snowden leak bares US spying on Philippines' text messages, The Phil Star Global, Available at: http://www.philstar.com/headlines/2014/05/20/1325354/snowden-leak-bares-us-spying-philippines-text-messages

38 Newsbytes Philippines, DOST exec named first commissioner of National Privacy Commission, 7 March 2016. Available at: http://newsbytes.ph/2016/03/07/dost-exec-named-first-commissioner-of-national-privacy-commission/ ; Newsbytes Philippines, Microsoft PH exec, lawyer-doctor appointed deputy chiefs at privacy agency, 9 March 2016. Available at: http://newsbytes.ph/2016/03/09/microsoft-ph-exec-lawyer-doctor-appointed-as-deputy-chiefs-of-privacy-commission/

Massive Breach of the Government's Electoral Commission

40. The COMELEC breach leaked online the personal information of approximately 55 million registered Filipino voters.[39] While some personal data in the tables (e.g., voters' names, birth dates, and Voter's Identification Numbers) were encrypted, others (e.g., residential address and birthplace) were not and could be easily ascertained. For Filipino voters registered overseas, there were cases wherein a person's birthplace, passport number, and the names of his/her parents could be identified by anyone familiar with the individual's real name.[40]

41. The immensity of the risk posed by the breach cannot be downplayed. Now recognized as one of the biggest breaches of government data in history,[41] it directed the public's attention to the extent of personal information being collected and held by Philippine government agencies, as well as their ability (or the lack thereof) to secure such information.

Bills seeking to establish a National ID System

42. Proposals to establish a national ID system have been filed by lawmakers at the House of Representatives,[42] as well as in the Senate[43]. The government will be mandated to issue a Filipino Identification Card for all Filipino citizens, which will include the owner's imprinted photograph, name, birth date, sex, date of issue, signature, and individual serial number as issued by the Philippine Statistics Authority. Without appropriate safeguards against the expansive surveillance capabilities of the government and the inability to secure against data breaches, there are concerns that this initiative increases significantly the risks to privacy being confronted by individuals.

39 Rappler, Comelec data leaked by hackers, 4 April 2016. Available at: http://www.rappler.com/nation/politics/elections/2016/127315-comelec-data-hackers

40 Bueza, M. and Manuel, W., Experts fear identity theft, scams due to Comelec leak, Rappler, 1 April 2016. Availble at: http://www.rappler.com/newsbreak/in-depth/127870-comelec-leak-identity-theft-scams-experts

41 Hern, A., Philippine electoral records breached in 'largest ever' government hack, The Guardian, 11 April 2016. Available at: https://www.theguardian.com/technology/2016/apr/11/philippine-electoral-records-breached-government-hack

42 Outgoing House Speaker and Quezon City 4th District Representative Feliciano Belmonte authored House Bill (HB) Number 12, whereas AKO Bicol (Party-List) Representatives RodelBacobe and Christopher Co co-authored HB Number 523, both titled the Filipino Identification System Act. Magdalo Party-List Representative Gary C. Alejano also filed a similar measure; see also: Cepeda, M., Lawmakers push for national ID system to reduce red tape, Rappler, 18 July 2016. Available at: http://www.rappler.com/nation/140089-house-bills-national-id-system and Philippine News Agency, More solons want Filipino ID system established, Manila Bulletin, 17 July 2016. Available at: http://www.mb.com.ph/more-solons-want-filipino-id-system-established

43 Senate Bills No. 69, 41, 15, and 917.

Recommendations

43. We recommend that the government of the Philippines:

- Review all laws, bills and policies to ensure that they comply with Philippines obligations to respect and protect the right to privacy under international human rights law;
- Take measures to ensure that provisions requiring judicial authorization of communication surveillance are respected and implemented;
- Ensure that all government authorities permitted to undertake communications surveillance are subject to independent oversight and comply with international transparency standards;
- Review the implementing rules and regulations of the Cybercrime Prevention Act of 2012 and take immediate steps (i.e., repeal or amend) as shall be determined by the reviewing body;
- Ensure that the Data Privacy Act is implemented and that the National Privacy Commission enjoys full independence and adequate resources to conduct of its functions;
- Conduct regular privacy audits on government agencies and offices processing personal data;
- Ensure that all government officers found to have contributed to the negligence that caused the COMELEC breach are held liable;
- Provide redress for human rights violations concerning the right to privacy by strengthening the National Privacy Commission's grievance and accountability mechanisms.