GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

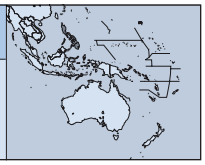
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

PHILIPPINES

Communications surveillance in the Philippines: Laws and the struggle for the right to privacy



Computer Professionals' Union
Rick Bahague
www.cp-union.com

Introduction

The Philippines has been crowned the "texting capital of the world"[1]the "social networking capital of the world",[2] and its financial district is ranked as the "selfiest city of the world".[3] Data is voluntarily uploaded and shared by its "netizens" on social media networks through mobile and landline networks and is a gold mine for any state surveillance activities. Its 106.5 million mobile subscribers sent two billion text messages daily last year. Fixed telephone subscription is almost non-existent, with a telephone density of four subscribers for every 100 inhabitants, and mobile subscriptions serve as the main communications tool. The digital divide has, however, plagued the country even after the deregulation of the telecommunications industry. The Philippines is ranked 98th in the world on the Information and Communications Technology Development Index (IDI),[4] with the lowest score compared to its Asian neighbours.

There are two monopolies controlling the telecommunications industry in the country: Globe Telecoms and Philippine Long Distance Telephone (PLDT). Telecommunications infrastructure is under the control of corporations. Government communications and transactions have to pass through this private network infrastructure, which is a concern for sensitive information. Because of this, most state surveillance activities would require some cooperation from any of the telecoms monopolies. In fact, the controversial "Hello Garci" wiretapping incident, which will be the focus of this report, was accomplished with the facilitation of one of their personnel.

Furthermore, the Philippines has been a longtime ally of the United States (US), being a former colony. Various agreements are in place which allow the US Armed Forces to use local resources for military exercises, to strategically position their weapons, and for mass surveillance activities. Edward Snowden revealed in March that the MYSTIC surveillance programme run by the US National Security Agency (NSA) monitors local telcos[5] and "scrapes mobile networks for so-called metadata – information that reveals the time, source, and destination of calls."[6]

While other governments in countries like Brazil and Germany protested the unlawful surveillance by the NSA, Philippine President Benigno Simeon "Noynoy" Aquino is not even familiar with the incident and has approved another agreement with the US on enhanced defence cooperation, which will open up more surveillance activities. In a statement, the Computer Professionals' Union (CPU) warned that the Enhanced Defense Cooperation Agreement (EDCA) "is an invitation for surveillance, drones and establishment of new listening posts violating rights to privacy and sovereignty."[7]

In this report, we look at the state of communications surveillance in the Philippines, focusing on government policies and how they were applied in a wiretapping incident. It remains to be seen if these policies can be used against the growing US military presence in the country.

1 Tuazon, J. M. (2012, December 4). 20 years on, SMS remains king in the 'texting capital of the world'. *Interaksyon*. Accessed July 17, 2014. www.interaksyon.com/infotech/20-years-on-sms-remains-king-in-the-texting-capital-of-the-world (20 years on, SMS remains king in the 'texting capital of the world'. Interaksyon)

2 MST Lifestyle. (2013, May 21). PH is social networking capital of the world. *Manila Standard Today*. manilastandardtoday.com/2013/05/21/ph-is-social-networking-capital-of-the-world

3 Golangco, V. (2014, March 13). Sexy and social: why Manila is the selfiest city in the world. *The Guardian*. www.theguardian.com/cities/2014/mar/13/manila-selfiest-city-most-selfies

4 International Telecommunication Union. (2013). *Measuring the Information Society 2013*. www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx

5 Robinson, K. (2014, May 22). 'NSA Gone Wild' in the Bahamas, Mexico, Kenya, the Philippines and more. *AccessNow.org*. https://www.accessnow.org/blog/2014/05/22/nsa-gone-wild-in-the-bahamas-mexico-kenya-the-philippines-and-more

6 Devereaux, D., Greenwald, G., & Poitras, L. (2014, May 19). Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas. *The Intercept*. https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas

7 Computer Professionals' Union. (2014, March 2). Enhanced defense cooperation: an invitation for surveillance, drones and unregulated communications. *Computer Professionals' Union*. www.cp-union.com/article/2014/05/02/enhanced-defense-cooperation-invitation-surveillance-drones-and-unregulated

Policies on communications surveillance

There are several policies governing surveillance, such as the Anti-Wiretapping Law, Cybercrime Law, Data Retention Law, Human Security Act, and E-Commerce Act. In addition, the National Telecommunications Commission has a standing Memorandum Circular for the retention of data by telecommunications companies.

The Anti-Wiretapping Act (AWA) enacted on 19 June 1969 is the first law regulating communications surveillance in the country. Section 1 of the AWA[8] specifically states: "It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device..." However, "any peace officer, who is authorised by a written order of the Court" upon a "written application and the examination under oath or affirmation of the applicant and the witnesses" can do this.

Before being granted authorisation, the AWA enumerates particular strict conditions that have to be met: (1) "that there are reasonable grounds to believe that any of the crimes enumerated [...] has been committed or is being committed or is about to be committed," (2) "that there are reasonable grounds to believe that evidence will be obtained essential to the conviction of any person for, or to the solution of, or to the prevention of, any of such crimes," and (3) "that there are no other means readily available for obtaining such evidence."

Furthermore, the AWA requires that authorisation should (1) identify the person or persons to be listened to, (2) identify the peace officer to overhear the communication, (3) identify the offence or offences committed or sought to be prevented, and (4) the period of authorisation. All conversations recorded are then to be submitted to the court within 48 hours after the expiration of the authorisation.

Section 3 of the Bill of Rights enshrined in the 1987 Philippine Constitution[9] guarantees every Filipino citizen the right to privacy of communication. It states: "(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." It specifically discourages authorities from conducting unlawful surveillance, otherwise: "(2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding." As such, the current Revised Penal Code penalises any unlawful entry, search or seizure carried out in violation of the Bill of Rights.

Republic Act 8792 or the Electronic Commerce Act of 2000[10] was the first law to govern electronic transactions in the age of internet in the country. It has a dedicated section (Section 31) on privacy or lawful access: "Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key."

On 6 March 2007, the Human Security Act (HSA)[11] was signed into law by former President Gloria Macapagal-Arroyo. Section 7 of the HSA specifically allows law enforcement agencies to "listen to, intercept and record, with the use of any mode, form, kind or type of electronic or other surveillance equipment or intercepting and tracking devices, or with the use of any other suitable ways and means for that purpose, any communication, message, conversation, discussion, or spoken or written words" between people identified by the government as "terrorists" – or even on the slight suspicion of being terrorists.

Five years later, the Cybercrime Prevention Act of 2012 (CPA 2012)[12] was signed by current President Aquino. Section 12 of the law gave law enforcement agencies the power to "collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system." In February 2014, the Supreme Court struck down this section of the CPA 2012 and ruled that real-time collection of network traffic violates the constitution.

A month before CPA 2012 was put into law, Aquino signed the Data Privacy Act of 2012 (DPA 2012). This law defined the rights of a "data subject" as well as the responsibilities of "data processors" to ensure privacy while "ensuring free flow of information to promote innovation and growth." It created the National Privacy Commission where all complaints on "unauthorised processing of personal

8 www.lawphil.net/statutes/repacts/ra1965/ra_4200_1965.html

9 www.gov.ph/constitutions/the-1987-constitution-of-the-republic-of-the-philippines

10 www.ipophil.gov.ph/images%5Cipenforcement%5CRA8792-E-Commerce_Act.pdf

11 www.congress.gov.ph/download/ra_13/RA09372.pdf

12 www.gov.ph/2012/09/12/republic-act-no-10175

information and sensitive personal information", "accessing personal information and sensitive personal information due to negligence", "improper disposal of personal information and sensitive personal information", among others, would be heard and processed. While there are no specific provisions on surveillance *per se*, the rights given to "data subjects" and prohibited acts are added safeguards against any kind of surveillance, in particular from the state.

As part of its regulatory function to protect users of telecommunications services, the National Telecommunications Commission also released a memorandum in 2007 on the data log retention of telecommunications traffic.[13] This memorandum is unnecessary from a privacy perspective, but was otherwise implemented. It "aims to further strengthen the welfare and protection afforded to end-users and/or consumers" by directing telcos to record and store voice and non-voice traffic for at least two months. To date, even with this memorandum, no one has been reprimanded for SMS spamming. This phenomenon is a common problem now, where advertisers use personal data collected illegally.

The "Hello Garci" wiretapping incident

It would take an alleged taped conversation of former President Arroyo during the 2004 elections to demonstrate that communications surveillance is happening in this country.

After the ouster of President Joseph Estrada in 2011, Arroyo, then vice-president, assumed office. Arroyo is perceived to be the most corrupt president of the republic.[14] IBON Foundation, a local think tank, estimated that PHP 7.3 billion (USD 181 million) of public funds were lost during her seven years in power.[15] In 2011, she would be charged with electoral fraud and plunder.[16].Among the popular evidence of her involvement in rigging the 2004 presidential election was a wiretapped conversation with an election commissioner which came to be known as the "Hello Garci Scandal".

A complete transcript of the wiretapped conversation[17] and a recording of the full conversation[18] are available on the website of the Philippine Center for Investigative Journalism (PCIJ). In this transcript, Arroyo called Commission on Elections (COMELEC) Commissioner Virgilio Garcillano (Garci) several times to ensure a lead of no less than one million votes against the popular rival Fernando Poe Jr. in the presidential race. She also made sure that documents to support this lead were consistent. In one conversation, she asked for the statement of votes (individual summary of votes from towns and municipalities) to make them consistent with the certificate of canvass (consolidated votes in the province).

The Hello Garci operation brought a 12-0 win for Arroyo's party in Lanao del Sur, a province in the southern island of Mindanao. In a Philippine election, voters select 12 senators in a ballot. It was an election manipulation operation which happened "with the complicity of the military, the COMELEC and even Malacanang,"[19] according to Sheila Coronel of the PCIJ. (Malacanang or Malacanang Palace is the official residence and office of the Philippine president.)

The wiretapped conversations were released on 6 July 2005 by no less than Presidential Spokesperson Ignacio Bunye. Arroyo addressed the nation in a televised speech on 27 June 2005 to apologise for the "mistake" of calling Garci and assured the people that she did not cheat in the previous election.[20]

The Hello Garci wiretapping incident was investigated by the Philippine Senate. It turns out that a military intelligence operation known as Project Lighthouse supervised the wiretapping of Garci and other individuals in the opposition. The Intelligence Services of the Armed Forces of the Philippines (ISAFP) working with personnel of a telco network made the wiretapping possible.[21]

The Hello Garci scandal exposed the manipulation of the most sacred right of the people in a democracy, elections. Furthermore, it also showed the current extent of communication surveillance performed by state forces.

13 Data Retention of Telecommunications Traffic, Memorandum Circular 04-06-2007, National Telecommunications Commission, 8 June 2007.

14 Gopalakrishnan, R. (2007, December 11). Arroyo "most corrupt" Philippine leader: poll. *Reuters*. www.reuters.com/article/2007/12/12/us-philippines-arroyo-idUSSP30281220071212

15 GMANews.TV. (2008, March 4). IBON: Corruption scandals under Arroyo cost Filipinos P7.3B. *GMANews.TV*. www.gmanetwork.com/news/story/83278/news/nation/ibon-corruption-scandals-under-arroyo-cost-filipinos-p7-3b

16 Associated Press. (2011, November 18). Philippines charges Gloria Arroyo with corruption. *The Guardian*. www.theguardian.com/world/2011/nov/18/philippines-asia-pacific

17 pcij.org/blog/2005/06/25/downloadables-section/3

18 pcij.org/blog/2005/06/25/downloadables-section

19 Coronel, S. (2005, November 2). Lanao's dirty secrets. *Philippine Center for Investigative Journalism*. pcij.org/stories/lanaos-dirty-secrets

20 A transcript of the president's speech is available on the PCIJ website: pcij.org/blog/2005/06/28/the-president-says-i-am-sorry-i-want-to-close-this-chapter-2

21 GMANews.TV. (2007, August 22). Doble: 'Hello Garci' wiretap ops done through Smart mole. *GMA News*. www.gmanetwork.com/news/story/57157/news/nation/doble-hello-garci-wiretap-ops-done-through-smart-mole

Surveillance of social movements

The Philippines has a vibrant protest and social movement. In 2001, technology played an important role in the ouster of President Joseph Estrada over allegations of corruption. TXTPower, a group composed of mobile subscribers, was active in the use of text messaging during the "Oust Erap Campaign" of various sectors ("Erap" was Estrada's nickname). It would also later launch a similar initiative against Arroyo.

Activists involved in social movements in the country are concerned with reports of electronic communication surveillance by state forces. The "Hello Garci" incident amplified these doubts. Moreover, the record of bringing justice to more than 1,206 victims of extrajudicial killings, 206 victims of forced disappearances, 2,059 victims of illegal arrests and 1,099 victims of torture during the Arroyo regime has been questioned in the second cycle of the Universal Periodic Review of the United Nations Human Rights Council.[22] The Philippine government is a signatory to the International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR) and the Universal Declaration of Human Rights.

If recent reports are to be believed, the current Aquino administration has purchased PHP 135 million (USD 3 million) worth of high-end surveillance equipment to spy on its critics.[23] This will be used by the ISAFP, which is alarming for social activists. ISAFP is the same agency that spearheaded the "Hello Garci" incident. It is now common activist practice that other than the usual personal security orientation, a discussion on information security is held so that they can take precautions.

Activists have also raised the alarm on the current regime's EDCA. For them, "allowing US troops to position equipment which will definitely include surveillance equipment and drones with free access to the radio spectrum is the best recipe for mass surveillance."[24]

This year, the Supreme Court nullified the real-time collection of data provision in the Cybercrime Act. This was declared unconstitutional, heeding the campaigns of the CPU and other netizen groups. However, libel, the most contested provision of the Act, which stifles freedom of expression, was upheld as within the frames of the constitution.

Violating the constitution and international norms

Wiretapping is a form of communications surveillance. The Philippines does not lack laws prohibiting and regulating it. The country's AWA and HSA are both a starting point for defining legitimacy, adequacy and necessity of surveillance. Both laws also have strict requirements for enforcement officers, which include authorisation from a judicial authority in the conduct of surveillance, due process and user notification. Moreover, any unauthorised surveillance is penalised with 10 to 12 years of imprisonment in the HSA.

While the Hello Garci incident exposed the rotten and corrupt system of the Philippine elections, it also demonstrated blatant disregard of the right to privacy and the 13 International Principles on the Application of Human Rights to Communications Surveillance.[25] It was conducted without court permission, due process or user notification, and revealed that telco companies and state authorities were working together. Until now, the intention of the wiretapping of Commissioner Garcillano which caught former President Arroyo by chance is unclear.

Even with existing laws legitimising communications surveillance, the practice remains problematic. The HSA, AWA and Cybercrime Act are widely opposed to too much power being given to the state. While judicial authority is required by these laws, opposition is still strong due to the doubtful impartiality of courts in issuing surveillance permissions.

Public oversight has yet to be seen in the implementation of the HSA. The law prescribes a Grievance Committee composed of the Ombudsman, the Solicitor General, and the undersecretary of the Department of Justice. The Committee is tasked to receive, investigate and evaluate complaints against the police and other state forces regarding the implementation of the law. An Oversight Committee, composed of senators and members of congress, has also yet to publish reports on its oversight functions.

Lack of integrity of communications and systems

Hello Garci was the first proof that the state and monopoly telcos are working together to track citizens.

22 Olea, R. (2012, May 21). Groups score continuing rights abuses as The Philippines and the Universal Periodic Reviewundergoes review by UN body. *Bulatlat*. Accessed July 17, 2014. http://bulatlat.com/main/2012/05/21/groups-score-continuing-rights-abuses-as-philippines-undergoes-review-by-un-body/

23 Tan, K. J. (2014, April 8). Palace backs ISAFP, denies using spy gadgets vs. opposition. *GMA News*. www.gmanetwork.com/news/story/355967/news/nation/palace-backs-isafp-denies-using-spy-gadgets-vs-opposition

24 Computer Professionals' Union. (2014, March 2). Op. cit.

25 https://en.necessaryandproportionate.org/text

It has created awareness among the general public that telcos and the government are tracking calls and text messages without court permission and user notification.

In the case of the Hello Garci incident, a special model of phone was used to receive calls diverted to it by the telco for recording.

Furthermore, a memorandum circular from the National Telecommunication Commission (NTC), the regulatory body overseeing telco monopolies, allows storage of voice and non-voice data supposedly to serve as reference for consumer complaints.[26] While intended for prosecution of consumer complaints, a similar section on real-time traffic monitoring in the Cybercrime Act was ruled as unconstitutional by the Supreme Court.

The Philippines is part of the NSA's MYSTIC and PRISM surveillance programmes

The country has more than a hundred years of being tied to the NSA in the US. In the early 1900s, in the great Philippine-American War, surveillance techniques were already employed. To defeat the Filipino guerrillas fighting for independence, the US army "created five integrated security agencies, a centralised telephone network, fingerprinting, photographic identification and index of police files of 200,000 alphabetised file cards with the means to collect, retrieve and analyse a vast amount of intelligence."[27]

Last March, Edward Snowden revealed that all text messages and calls passing through the two telco monopolies in the Philippines are captured by the NSA. With more than 100 million users of mobile telephones, and a vibrant protest movement which is demonised for its militancy, the US has all its reasons to implement mass surveillance in the country. In 2013, Snowden also said that the NSA has an established listening post in Manila to conduct mass surveillance against other Asian countries.

Recently, a new agreement with the US was signed by the Department of Foreign Affairs. The EDCA allows US weapons to be based in the country. The US has a rotating military presence through its frequent military exercises allowed by the Visiting Forces Agreement (VFA). The EDCA has been studied by a group of computer professionals and was found to be "an invitation for unregulated communication and surveillance" due to its provision of allowing US troops to use the full radio spectrum, which is heavily regulated by the National Telecommunications Commission.

Conclusions

The Philippines has established laws on communications surveillance since 1969. Its constitution also regards privacy as a fundamental right of its citizens. In the Hello Garci scandal, where former President Arroyo was caught as she allegedly instructed Commissioner Garcillano – who was being wiretapped by the intelligence agency of the armed forces – to rig the 2004 presidential election in her favour, the right to privacy and the principles of judicial authority, due process and user notification were not applied. This also verified the fears of activists and privacy advocates on the possible connivance between telcos and state forces to track electronic communications.

Furthermore, the country has a long history of being part of NSA spy programmes. Its previous and present administrations have been subservient to US interests, which includes allowing the establishment of listening posts by the NSA to establish listening posts, the capture of massive amounts of metadata on mobile networks, and the importing of surveillance equipment through the EDCA and VFA.

However, Filipino netizens are also aware of their political strength, once mobilised. They were active in the ouster of two previous presidents and have shown their capacities again in the 2013 Million People March against the corrupt use of public funds by the current Aquino regime. It did not take long before they realised that the state and the US had been tracking their activities online and offline.

Action steps

The following recommendations can be made so that awareness of the 13 Principles and a stronger sense of the right to privacy are propagated:

- Through campaigns, create awareness of the Snowden revelations and how the state and telcos have cooperated with the NSA to conduct communications surveillance.
- Lobby for an Internet Bill of Rights similar to Brazil's.
- Call for the strict implementation of the Data Privacy Act to protect citizens from the misuse of data for profit.
- Create forums on information security and privacy rights, similar to CPU's briefing for social activists.

26 Data Retention of Telecommunications Traffic, Memorandum Circular 04-06-2007, National Telecommunications Commission, 8 June 2007.

27 Morey, M. (2013, June 25). From Philippines to NSA: 111 years of the U.S. surveillance state. *Occupy.com*. www.occupy.com/article/philippines-nsa-111-years-us-surveillance-state