UNIVERSITY OF TORONTO

Supporting South-based cyber security scholars, advocates, and practitioners.

CYBERSTEWARDS

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Foundation for Media Alternatives
The Citizen Lab

Research Brief
March 2017

An Overview of Internet Governance and Infrastructure in the Philippines

COUNTRY CONTEXT

The Republic of the Philippines is an archipelago of more than 7,100 islands spread over 300,000 square kilometres, with a population of more than 100 million people. After a 425-year history of colonialism and a traumatic period of authoritarianism (that ended in 1986), the country has emerged as a democracy that continues to experience political upheaval and economic boom and bust.

The Philippines has been ruled by a succession of political dynasties, many of whom also dominate the economy, including the media and information and communications technology (ICT) industry. As a result, the ICT sector is underdeveloped, with only two major telecommunications companies dominating the market. Poverty is pervasive, and wide income disparities exist despite recent economic growth. Challenges from armed communist rebels and Muslim separatists persist, while a restive military retains its influence over the country's political life. At the same time, however, Philippine civil society is one of the most vibrant in the world. It is consistently advocating for good governance, sustainable development, socio-economic and political reforms, and human rights.

The Philippines formally connected to the Internet in 1994, but even today the Internet remains largely unregulated.[1] While national plans champion ICTs for their socio-economic potential, governance has been unevenly distributed because of limited state capacity and resources, and regulatory capture by dominant market players. It comes as no surprise that the access rate for the majority of the population remains low, with estimates for Internet usage hovering at about 40% of the population. Mobile penetration is high at 101%,[2] and yet at 30%, smartphone penetration in the Philippines is relatively low.[3] (See Table 1 for key ICT indicators.)

[1] Sec. 3(h) of the country's *Republic Act 7925* defines a value-added service provider as "an entity which, relying on the transmission, switching and local distribution facilities of the local exchange and inter-exchange operators, and overseas carriers, offers enhanced services beyond those ordinarily provided for by such carriers."

[2] Ezra Ferraz, "New Study Predicts Smartphone Penetration in the Philippines Will Triple by Next Year," *Tech in Asia*, 4 August 2014, https://www.techinasia.com/philippines-mobile-smartphone-penetration/.

[3] "Survey: PH Smartphone Penetration Rate at 15%," *Newsbytes Philippines*, 18 September 2013, http://newsbytes.ph/2013/09/18/survey-ph-smartphone-penetration-rate-at-15/.

TABLE 1. Selected Philippine ICT Indicators	
Population (January 2016)	101.47 million
Internet penetration (March 2015)	44.2 million or 44% of population
Growth of Internet population (2009–2013)	531%
Active social media users (January 2016)	48 million or 47% of population
Mobile connections/subscriptions (January 2016)	119.21 million or 117% of population
Active mobile social media users (January 2016)	48 million or 47% of population
Active Internet users (January 2016)	47.13 million or 46% of population
Mobile penetration (January 2016)	75.4 million or 74% of population
Percentage of mobile connections that are pre-paid (January 2016)	95%
Percentage of mobile connections that are post-paid	5%
Percentage of mobile connections that are broadband (3G and 4G)	47%
Fixed broadband subscriptions (2014)	23.2 million
Wireless broadband penetration (2014)	27%

Sources: We are Social January 2016;[4] Internet Society Global Internet Report 2014;[5] World Bank Indicators 2014;[6] ITU World Telecommunications ICT Indicators Database 2014;[7] *Global Web Index*. March 12, 2014.[8]

By law (*Republic Act No. 7925*), Internet service delivery is anchored on telecommunications networks that, in turn, are controlled almost exclusively by two monolithic companies: the Philippine Long Distance Telephone Company, or the PLDT group—which also owns providers such as Smart, Talk n Text, and Sun Cellular—and Globe Telecom, Inc. These two companies also own most of the Internet infrastructure in the country, allowing them to dictate the cost, quality, and extent of Internet connectivity.[9]

Entering the country's telecommunications industry is a cumbersome process. Anyone interested in conducting such a business must first obtain a franchise through Congress.[10] The constitution mandates that telecommunications firms—considered a public utility—must be principally owned (60%) by Filipino nationals.[11] On top of that, various other licences and permits from different government agencies, including local government units, must be secured. Globe Telecom's senior vice president for technical services, Emmanuel Estrada, said that telecommunication companies "need to secure an average of twenty-five permits at the local government level"—a process that takes at least eight months to complete—to build a single cell site.[12] Philippine's Internet, however, has been able to thrive in such a limited environment. The country was

[4] "Digital in 2016," We Are Social, 26 January 2016, http://www.slideshare.net/wearesocialsg/digital-in-2016/321.
[5] "Global Internet Penetration," Internet Society, http://www.internetsociety.org/map/global-internet-report.
[6] "Indicators," World Bank 2014, http://data.worldbank.org/indicator.
[7] International Telecommunications Union, www.itu.int.
[8] Jason Mander, "As the Internet Turns 25, China Has 2.5 Times More Users Than US," Global Web Index (blog), 12 March 2014, http://www.globalwebindex.net/blog/internet-turns-25.
[9] Mary Grace Mirandilla-Santos, "Philippine Broadband: A Policy Brief," Policy Brief No. 4, February 2016.
[10] RA 7925, article 6, §16.
[11] Section 11, article 12 of the 1987 Philippine Constitution.
[12] Jeandie O. Galolo, "Gov't Setup, Not Competition, Will Improve Internet Speed," *Sun Star/CEBU*, 19 April 2016, http://www.sunstar.com.ph/cebu/business/2016/04/20/govt-setup-not-competition-will-improve-internet-speed-468842.

dubbed the "text messaging capital of the world" in the early 2000s,[13] and has been known as the global "social media capital"[14] and "selfie capital."[15]

This report outlines the overarching ICT infrastructure and existing governance mechanisms, as well as general trends in the country's ICT policy and Internet governance arena, including civil society's recent key issues and those that currently require the most attention. We also present network measurement testing results and analysis. The report includes some scenarios to anticipate particular points of intervention by public interest organizations, especially with the recent transition to a new administration in July 2016.

INFRASTRUCTURE AND GOVERNANCE

Telecommunication Companies

PLDT and Globe, the two major network operators in the country, control 83% of the local market. Sun Cellular, a joint venture between Singapore Telecommunications Ltd. and local outfit Ayala Corporation, ranks third in significance.

As of 2012, there were already over 350 Internet Service Providers (ISPs) in the country.[16] Most of these ISPs connect through PLDT's network, which owns the majority of fixed-line connections, as well as a 100,000-kilometre fiber network that makes it the most extensive in the country.[17] The government's planned launch of free Wi-Fi services targeted half of its cities and municipalities over the course of 2015,[18] with the goal of expanding the service with the help of increased funding in 2017.[19] In 2015, the arrival of a third telco, which was to consist initially of a joint venture between Telstra (Australia's largest telco) and San Miguel Corporation (Philippines' largest food, beverage, and packaging company) was reported.[20] However, in March 2016, negotiations between San Miguel Corporation and Telstra were terminated.[21]

PLDT's history dates back to 1932, when the then-colonial Philippine Congress granted it a fifty-year franchise to operate a national telephone system. The company's initial management consisted of Americans, although the major stakeholder was a Canadian company called British Columbia Telephone. In 1956, BC Telephone sold its stake to an American company, General Telephone and Electronic Corporation (GTE).[22] It

[13] Josefina T. Lichauco, "The Philippine Text Messaging Phenomenon," *The Philippine Star*, 15 May 2001, http://www.philstar.com/business-life/85823/philippine-text-messaging-phenomenon.
[14] "Research Confirms: The Philippines is Still the Social Media Capital of the World," *Yahoo News*, 2 July 2014, https://sg.news.yahoo.com/research-confirms-philippines-still-social-033045566.html.
[15] Chris Wilson, "The Selfiest Cities in the World: *Time*'s Definitive Ranking," *Time Magazine*, 10 March 2014, http://time.com/selfies-cities-world-rankings/.
[16] *Philippines in Figures 2014* (Quezon City: Republic of the Philippines National Statistics Office, 2014), https://psa.gov.ph/sites/default/files/2014%20PIF.pdf.
[17] "PLDT Acquires 'Metro Fone' and Expands its Fixed Line Coverage in Philippines," *Telecom Drive*, 6 June 2015, http://telecomdrive.com/pldt-acquires-metro-fone-and-expands-its-fixed-line-coverage-in-philippines/.
[18] Tom Huddleston, Jr., "Philippines to roll out nationwide free WiFi by 2016," *Fortune*, 8 September 2015, http://fortune.com/2015/09/08/philippines-free-wifi/.
[19] "P1.76B earmarked for free Wi-Fi in proposed 2017 budget," *Rappler*, 4 September 2016, http://www.rappler.com/business/governance/145175-philippines-free-wifi-public-areas-dict-2017-budget.
[20] Grace In Mono, "Impending Telstra-SMC Partnership Puts Pressure on PH Telecom," *Telecomasia* (blog), 26 October 2015, http://www.telecomasia.net/blog/content/impending-telstra-smc-partnership-puts-pressure-ph-telecom.
[21] Louella Desiderio, "San Miguel-Telstra Joint Venture Talks Terminated," *The Philippine Star*, 15 March 2016, http://www.philstar.com/business/2016/03/15/1562973/san-miguel-telstra-joint-venture-talks-terminated.
[22] Lorraine Carlos Salazar "Getting a Dial Tone: Telecommunications Liberalisation in Malaysia and the Philippines," Institute of Southeast Asian Studies (2007), 102.

was not until 1968 when a group of Filipino businessmen bought GTE's stake that PLDT finally became a Filipino-controlled corporation.[23]

In the 1990s, under the leadership of President Fidel Ramos, the government liberalized the telecommunications industry. Through telephone policy, the NTC created a "service area scheme" that divided the country into eleven service areas. Cellular phone companies were mandated to expand the national infrastructure by installing 400,000 lines in three years, while international carriers were to install 300,000 in five years.[24]

The Public Telecommunications Act (RA 7925) was enacted in 1995 and institutionalized liberalization and competition. The act designated the NTC as the main regulatory power over all telecom services, and the Department of Transportation and Communication (DOTC) as the agency responsible for developing a long-term national development plan for the industry.[25] By 1998, teledensity had risen from 1.0 telephone connections per 100 people in 1991 to 9.08, and the cost per minute of national and international calls had decreased by 66%. With nine international gateway facilities, five cellular mobile phone providers, and fourteen paging companies, consumers had, at one point, a wide set of service providers to choose from.[26]

With the absence of anti-trust laws up until 11 June 2015 when the Philippine Competition Act was ratified by Congress,[27] PLDT managed to retain its dominance through a series of mergers and acquisitions. In 2011, for instance, PLDT acquired a majority interest in its direct competitor, Digital Telecommunications Philippines, Inc. (Digitel). Estimates suggested that the transaction resulted in PLDT controlling two-thirds of the mobile market.[28] Globe Telecom and consumer groups opposed the deal, but it went ahead, and thus gave PLDT 98% control of Digitel.[29] On 21 July 2015, Globe raised its ownership in Bayan Telecommunications Inc. from 56.87% to 98.57%.[30] Predictably, PLDT and its affiliates opposed the move and argued that the transaction would "lead to Globe's acquisition of a grossly disproportionate amount of frequencies in relation to their subscriber base."[31]

Internet Connectivity

There are six domestic Internet Exchange Points (IXPs) in the Philippines, with the Open Internet Exchange (PHOpenIX) acting as a "neutral" Internet exchange that is managed and operated as a nonprofit by the Department of Science and Technology. However, there remains a lack of interconnectivity between the major ISPs. As a result, an estimated 97% of local traffic[32] is routed externally through places such as Hong Kong and the United States before returning to the country, which causes delays in data transmission and slows

[23] "Enabling the Nation," PLDT Company Timeline, http://www.pldt.com/about-us/company-timeline.
[24] "Getting a Dial Tone," 248.
[25] Ibid., 307.
[26] Mary Ann Reyes, "PLDT: From Voice to Multi-media," *The Philippine Star*, 22 October 2012, http://www.philstar.com/business-usual/2012/10/22/859665/pldt-voice-multi-media-first-two-parts.
[27] Chris Schnabel, "What Consumers Need to Know About the PH Competition Act; Part 1: The Measure Aims to Give Consumers More Choices and Lower Prices Through Stronger Market Competition," *Rappler*, 9 July 2015, http://www.rappler.com/business/economy-watch/98287-philippine-competition-act-part-1.
[28] Matt Ablott, "Philippines Mobile Market Becomes Two-horse Race," GSMA Intelligence (research note), 24 May 2012, https://gsmaintelligence.com/research/2012/05/philippines-mobile-market-becomes-two-horse-race/336/.
[29] "PLDT Now Owns 98% of Digitel," *Rappler*, 19 January 2012, http://www.rappler.com/business/976-pldt-now-owns-98-of-digitel.
[30] Louella D. Desiderio, "Globe Buys out Lopez Group in Bayantel," *The Philippine Star*, 22 July 2015, http://www.philstar.com/business/2015/07/22/1479459/globe-buys-out-lopez-group-bayantel.
[31] Ibid.
[32] "NTC Drops Mandatory ISP Interconnection [The Manila Times, Philippines]," *NFV Zone News*, 29 August 2011, http://www.nfvzone.com/news/2011/08/29/5738498.htm.

down Internet access.[33]

In an effort to boost connectivity, the NTC in 2011 instructed ISPs to interconnect using PHOpenIX. The telcos were heavily opposed to this, with PLDT citing the security of its Internet traffic as one of its concerns.[34] They did not stand down even when the NTC revised its directive to simply require all ISPs with direct connection to a foreign ISP to negotiate and agree to interconnect their IP exchanges.[35] PLDT contested the NTC's directive by arguing that interconnectivity will allow smaller ISPs to "free ride" with those who have made greater investments in infrastructure.[36]

The NTC faces challenges in dealing with ISPs because the Philippines considers the Internet as a deregulated "value-added" service.[37] Value-added services, unlike telecom services, are not subject to government regulation. Unless it puts up its own network, a telecommunications entity operating as a value-added service provider is subject to only a few requirements imposed by law.[38] Accordingly, the NTC as the primary regulator has no power to impose IP peering (a voluntary process in which two Internet networks connect and exchange traffic).[39] As a result, IP peering in the Philippines is a commercial affair, in which ISPs charge other providers who want to connect to them. Meanwhile, in other countries such as Indonesia, telcos and ISPs are peered for free.[40]

On 16 September 2014, in a senate hearing held on the subject of peering, Globe Telecom backed NTC's position on mandatory IP peering.[41] PLDT, on the other hand, was reluctant to show its support.[42] In an agreement signed in September 2015 with the Department of Science and Technology's Information and Communications Technology Office (ICTO), PLDT agreed to connect to the PHOpenIX, which has been designated as the official Government Internet Protocol Exchange (G/IPX).[43] Signing the agreement did not mean, however, that PLDT had finally relented on its position against peering. Government policy dictates that all government agencies must "exchange data traffic with other government agencies and external stakeholders" through the G/IPX facility.[44] Thus, by connecting to the PHOpenIX, PLDT had fulfilled the requirement to be part of local IP peering, and could keep its government contracts. It could also bid for other government Internet-related projects, such as the nationwide free Wi-Fi project.[45] Globe, for its part, claimed that the government has not done enough to markedly improve Internet speed in the country. It noted that the policy requires PLDT clients to peer with government websites only, but does not require PLDT to exchange

[33] Darwin G. Amojelar, "PLDT, Globe at Odds Over Proposed Revival of IP Peering Policy," *InterAksyon*, 2 June 2014, http://www.interaksyon.com/business/88136/pldt-globe-at-odds-over-proposed-revival-of-ip-peering-policy.
[34] "ICT Office to Sign Deal with PLDT as Third PH Internet Exchange Connection," *Newsbytes Philippines*, 2 September 2015, http://newsbytes.ph/2015/09/02/ict-office-to-sign-deal-with-pldt-as-3rd-ph-internet-exchange-connection/.
[35] "NTC Drops Mandatory ISP Interconnection [The Manila Times, Philippines]," *Next Generation Communications News*, 30 August 2011, http://next-generation-communications.tmcnet.com/news/2011/08/29/5738498.htm.
[36] "PLDT: We're Operating and Supporting Voluntary IP Peering," *Newsbytes Philippines*, 7 July 2014, http://newsbytes.ph/2014/07/07/pldt-were-operating-and-supporting-voluntary-ip-peering/.
[37] A value-added service is all service beyond standard voice calls and fax.
[38] *Republic Act No. 7925*, §11.
[39] "What Is Peering?" Netnod, http://www.netnod.se/ix/what-is-peering.
[40] Carmela Fonbuena, "Pressure on PLDT to Solve PH's Slow Internet," *Rappler*, 16 September 2014, http://www.rappler.com/business/industries/215-tech-biz/69279-ip-peering-pldt-pressure.
[41] "PLDT Rejects IP Peering Proposal of NTC, Globe," *GMA News Online*, 10 August 2011, http://www.gmanetwork.com/news/story/229056/scitech/pldt-rejects-ip-peering-proposal-of-ntc-globe.
[42] "PLDT to Globe: You Got It Wrong on Domestic IP Peering," *Newsbytes Philippines*, 15 July 2014, http://newsbytes.ph/2014/07/15/pldt-to-globe-you-got-it-wrong-on-domestic-ip-peering/.
[43] "ICT Office to Sign Deal with PLDT as 3rd PH Internet exchange connection," *Newsbytes Philippines*, 2 September 2015, http://newsbytes.ph/2015/09/02/ict-office-to-sign-deal-with-pldt-as-3rd-ph-internet-exchange-connection/.
[44] Administrative Order No. 39, s. 2013, http://www.gov.ph/2013/07/12/administrative-order-no-39-s-2013/.
[45] "PLDT Promises Faster Loading Gov't Websites," *Rappler*, 8 September 2015, http://www.rappler.com/technology/news/105158-pldt-ip-peering-phopenix-govt-sites.

traffic with other ISPs.[46]

Internet Access

Although access to ICTs has been steadily rising — due primarily to affordable smartphones — Internet speeds provided to Philippine consumers are among the worst in the world, while prices for such services remain high.[47] Many attribute this to the virtual oligopoly of the two major telcos.[48] While most urban centres find themselves wired to the Internet, access in remote communities, particularly in far-flung mountainous and small island communities, is still underdeveloped. Most of the country's public schools are still not online,[49] while vulnerable groups — indigenous people, individuals with disabilities, and the rural poor — continue to struggle with affordability and accessibility issues. Women's groups have recently convened to advocate for improvements to gender-related access to ICTs in the Philippines.[50]

BOX 1. Gender, ICTs, and Public Policy

In recent years, issues of technology-related violence against women (VAW) have been reported in the media and to law-enforcement agencies. They have included cases of identity theft, uploading of images and videos without consent, hate speech on the basis of one's sexual orientation, gender identity, expression (SOGIE), and cyber harassment. While laws in relation to these have been enacted (i.e., the Anti-Photo and Video Voyeurism Act), they represent but a portion of the issues women have had to deal with.

Access to the Internet, especially by women in the rural and remote areas of the country, is a pressing concern in the Philippines. Other sectors (e.g., indigenous people, those with disabilities, and poor women) may also be losing out on opportunities because they lack access to the Internet.

A recent study by the Foundation for Media Alternatives on women's empowerment through the Web identified barriers to women's use and access that included affordability issues, not having time to use the Internet, or simply not knowing how.[51] Digital literacy and content development for women were seen as crucial in addressing some of these barriers. It is also important to look into existing government policies in relation to ICTs and see how these affect women, or if women were considered and consulted during policy development.

[46] "Globe Scoffs at PLDT Peering Deal with Gov't Internet Exchange," *Newsbytes Philippines*, 27 September 2015, http://newsbytes.ph/2015/09/27/globe-scoffs-at-pldt-peering-deal-with-govt-internet-exchange/.
[47] See Matikas Santos, "PH Has Slowest Internet in Southeast Asia," *Inquirer*, 21 April 2014, http://technology.inquirer.net/35596/ph-has-slowest-Internet-in-southeast-asia; Lila Shahani, "Why Is Our Internet So Slow?" *The Philippine Star*, 24 August 2015, http://www.philstar.com/opinion/2015/08/24/1491398/why-our-Internet-so-slow. It is said that the average prices for monthly Internet subscription in the country is three times higher than the global mean.
[48] See, for example, Grace Mirandilla-Santos, "State of PH Internet: Access, Quality and Cost" presentation to the senate of the Philippines in 18 August 2015. A recent roundtable convened by the American Chamber of Commerce in the Philippines on 3 December 2015 reached the same conclusions.
[49] See the Asian Institute of Journalism and Communication, "Survey on Internet Use and Access by Philippine School Children," http://dev2.websiteexpress.ph/aijc/wp-content/uploads/2015/05/survey_internet_access.pdf.
[50] Proceedings of the "Real Access for Women: A National Consultation on Gender and ICT" (8 and 9 December 2015, Oracle Hotel and Residences, Quezon City). Convened by FMA in partnership with other CSOs.
[51] "Women's Rights Online: Translating Access into Empowerment," World Wide Web Foundation, Philippine Report, FMA, August 2015, http://webfoundation.org/about/research/womens-rights-online-2015/.

Recent ICTO initiatives, such as its initial forays into Internet connectivity via TV White Space (TVWS) and Free Public Wi-Fi, are laudable but not without problems.[52] Regulatory issues abound in TVWS, and the Wi-Fi program has had difficulty getting off the ground because of delays and other issues in the procurement process.[53]

Affordable and reliable access is now considered a right. In 2015, it was included in the *Philippine Declaration on Internet Rights and Principles*, a civil society initiative seeking to create a rights-based framework for Philippine Internet.[54] Some of the policies proposed by the *Declaration* aim to address many of the anticompetitive loopholes that currently exist in the telecommunications industry.

There is also no strategic universal access strategy for the country, a lack best exemplified by the much-delayed National Broadband Strategy that the ICTO was supposed to formulate years ago. The Philippines pays lip service to affordable access, but struggles to put in place many basic elements of this access. The absence of an overall access strategy is troubling because the access regulatory puzzle is also being affected by other content-related concerns—either traditional (e.g., licensing issues under strict "intellectual property" regimes or "access to knowledge" rights) or emergent (e.g., debates on "net neutrality" are evident in issues such as zero-rating and offerings such as Facebook's Internet.org). There is also an absence of a national digital literacy program, often considered to be an important partner program to Internet access.

Barriers to Access

The Philippines' archipelagic geography poses a huge challenge to the development of a robust ICT infrastructure. Connecting more than 7,000 islands—some with remote mountain and coastal communities—has been difficult even for the country's incumbent telco operators. Other barriers include low income among the population. The country also needed a central government agency to oversee ICT development. Of the ten members of the Association of Southeast Asian Nations (ASEAN), it has consistently ranked sixth in terms of ICT connectivity since 2010, trailing behind Singapore, Brunei Darussalam, Malaysia, Thailand, and Vietnam.[55] The World Economic Forum's Networked Readiness Index ranks the Philippines seventy-sixth out of 143 countries in terms of its capacity to prepare for, use, and leverage ICTs.[56]

The Philippines has had the fastest growing Internet population in the world, experiencing 531% growth over the last five years,[57] resulting in 47.1 million active Internet users as of January 2016.[58] This growth, however, has not been accompanied by a similar increase in ICT infrastructure. According to *Ookla's Household Download Index*,[59] the country has one of the slowest average broadband speeds in the world. Ookla's test

[52] See "Free Wi-Fi Internet Access in Public Places," Department of Science and Technology Information and Communications Technology Office, www.dict.gov.ph/wp-content/uploads/2015/03/Free-Wi-Fi-Project-TOR.pdf.
[53] Marvin Sy, "Miriam Seeks Review of DOST Public Wi-Fi Project," *Philippine Star*, 26 September 2015, http://www.philstar.com/headlines/2015/09/26/1504060/miriam-seeks-review-dost-public-wi-fi-project; also "Miriam Hits Underspending at ICT Office, Wants Wi-Fi Project Completed Soon," *Newsbytes Philippines*, 28 September 2015, http://newsbytes.ph/2015/09/28/miriam-hits-underspending-at-ict-office-wants-wi-fi-project-completed.
[54] Information and Communication Technology Office, "Launch of the Philippine Declaration on Internet Rights and Principles," Republic of the Philippines Department of Information and Communications Technology, www.dict.gov.ph/launch-of-the-philippine-declaration-on-internet-rights-and-principles/.
[55] Jose Ramon G. Albert and Raymond E. Gaspar, "What Do ICT Stats Say About the Philippines?" *Rappler*, 22 April 2015, http://www.rappler.com/thought-leaders/90584-ict-statistics-philippines.
[56] "Network Readiness Index," World Economic Forum, http://reports.weforum.org/global-information-technology-report-2015/network-readiness-index/.
[57] Phoebe Magdirila, "Philippines Records the Biggest Internet Population Growth Globally," *Tech in Asia*, 13 March 2014, https://www.techinasia.com/philippines-records-biggest-internet-population-growth-globally/.
[58] "Internet Use, January 2016," Slide Share, We Are Social, http://www.slideshare.net/wearesocialsg/digital-in-2016/310.
[59] http://www.netindex.com/ (Site discontinued).

data between 18 April 2015 and 17 May 2015 showed a household download speed of 3.64 megabit per second (Mbps), the second lowest among Asian countries in the Index. It ranked the Philippines at 176 out of 202 countries as of May 2015. The only Asian country with a lower download speed was Afghanistan, at 2.52 Mbps.[60]

In terms of upload speed, the Philippines ranked even lower on the index with an average upload speed of 1.53 Mbps. (The global average is 10.59 Mbps.) Cost per Mbps was also one of the world's most expensive, with an average value of USD 18.18 compared to the global average of USD 5.21.[61] It thus comes as no surprise that a survey by *On Device Research* showed that one-fourth of respondents were dissatisfied with the quality of their Internet services.[62]

In 2014, the underwhelming state of the country's Internet caused lawmaker Rep. Mark Villar to file House Resolution 1658, which prompted the House of Representatives' Committee on Information and Communication Technology to conduct an inquiry.[63]The Department of Justice (DOJ) also warned telcos against deceiving consumers in their advertisements.[64] The NTC, for its part,[65] grilled major telcos in a public consultation on 7 November 2014 regarding the minimum speed of their broadband connections.[66] Since then, it has pushed for legislation that would identify broadband as an essential service to justify government regulation.[67] It has also supported proposals that seek to impose penalties against telcos that provide substandard services.[68]

Telcos, meanwhile, have argued that the government's complicated licensing process is actually at fault.[69] Telcos are required to secure over twenty permits from local government units (LGUs)[70] before a cell tower site is cleared for construction. In a senate hearing on the impact of slow and expensive Internet connections, representatives from both *Globe Telecom* and *PLDT* raised the issue of bureaucratic red tape as an industry-wide concern and urged LGUs to follow standard and transparent procedure in dealing with telcos.[71]

LAWS AND REGULATIONS

The Philippine government recognizes the important role of ICTs in people's lives. The 1987 constitution establishes the framework for the state's responsibility in harnessing the potential of ICTs. It states that the government recognizes the vital role of communication and information in nation building, and declares

[60] "Guess Which Asian Country Has Slower Internet Than PH?" *ABS–CBN News*, 19 May 2015, http://www.abs-cbnnews.com/business/05/19/15/guess-which-asian-country-has-slower-internet-philippines.
[61] Ibid.
[62] "The Philippines Mobile Internet Crowd: Young, Affluent, and Growing Fast," *On Device Research* (blog), 8 July 2014, https://ondeviceresearch.com/blog/philippines-mobile-internet-trends.
[63] Patricia Lourdes Viray, "House Inquiry on Slow Internet Connection Sought," *The Philippine Star*, 26 December 2014, http://www.philstar.com/headlines/2014/12/26/1406673/house-inquiry-slow-internet-connection-sought.
[64] April Lastimoza, "DOJ Warns Telcos Not to Deceive Consumers with 'Unlimited Internet' Promos," *Kicker Daily News*, 12 December 2014, http://kickerdaily.com/doj-warns-telcos-not-to-deceive-consumers-with-unlimited-internet-promos/.
[65] "Mandate, Vision, Mission," NTC, http://ntc.gov.ph/mandates.php/?page_id=970.
[66] "Telcos to Explain Expensive but Slow Internet at NTC Hearing," *Rappler*, 20 October 2014, http://www.rappler.com/business/industries/172-telecommunications-media/72568-ntc-public-hearing-internet-speed.
[67] Ibid.
[68] Darwin G. Amojelar, "NTC Readies Fines vs. Poor Internet Service," *Manila Standard*, 5 April 2015, http://manilastandardtoday.com/2015/04/05/ntc-readies-fines-vs-poor-internet-service/.
[69] Mick Basa, "Slow Internet? Blame Red Tape—Telcos," *Rappler*, 28 January 2015, http://www.rappler.com/business/industries/172-telecommunications-media/82208-slow-internet-blame-red-tape.
[70] Local government units refer to the different local governments in the Philippines. They are divided into three levels: (1) provinces and independent cities; (2) component cities and municipalities; and (3) barangays. They enjoy some degree of autonomy from the national government, although the President retains general supervisory powers.
[71] Basa, "Slow Internet?"

science and technology essential for national development and progress.[72] It also tasks the state to *"regulate the transfer and promote the adaptation of technology for the national benefit*,"[73] thereby placing policy development and governance of ICTs well within the state's ambit of interest. Yet the government has been inconsistent in its implementation of this mandate. The local political context, internal capacity issues, and shifting realities that affect ICT policy and Internet governance are but a few of the underlying reasons.

The Internet's existence has necessitated a re-imagination of previous governance paradigms. Just as all sectors are being forced to catch up to the opportunities presented by these developments, the ICT policy ecosystem is also experiencing difficulties keeping up. This difficulty became apparent in the debates relating to the World Conference on International Telecommunications (WCIT) in December 2012.[74] During the discussions to revise the International Telecommunication Regulations (ITRs), the disagreements between country delegations became so heightened that they eventually led to unprecedented divisions between the parties, all of whom were trying to determine how to properly treat Internet service within telecom-centric paradigms.[75] With ICTO as the lead of the delegation to the event, the Philippines opted not to sign the agreement arrived at during the forum. It cited its need to consult its stakeholders before agreeing to sign the accord, which it believed had the potential to negatively affect the local business process outsourcing sector. It also pursued a broader view of telecom regulation to include services, although this view was not shared or adopted by other government agencies.[76]

Technology has outpaced policy on many levels. This situation has sometimes led to confusing and even conflicting policy responses from government. With social media, for example, government agencies have had different views on how the state should regulate—and even use—social media tools.[77] When the *Cybercrime Protection Act* was put forward, there was a clash between online regulation and Internet rights, particularly on the issue of online libel. When the Supreme Court was forced to decide on the act's constitutionality,[78] Internet policy-making was essentially left in the hands of elderly justices, few of whom understood the complexities of cyberspace. The Supreme Court eventually ruled that the controversial provision on online libel is constitutional, a decision that many netizens protested by posting tweets using the #NonLibelousTweet hashtag.[79]

The same may be said of another controversial case involving high-school students of an all-girls school who posted their bikini photos on their Facebook accounts. The case was decided by the Supreme Court a few

[72] 1987 *Philippine Constitution*, sec. 10, art. XIV.
[73] 1987 Philippine Constitution, sec. 12, art. XIV.
[74] See World Conference on International Telecommunications (WCIT-12), http://www.itu.int/en/wcit-12/; for an overview of some of the issues surrounding WCIT, for example, "After WCIT—Where Do We Go from Here?" Internet Society, http://www.Internetsociety.org/wcit.
[75] See a summary of the country positions by Mike Masnick, "Who Signed the ITU WCIT Treaty, and Who Didn't," *Tech Dirt,* 14 December 2012, https://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml.
[76] For the first time in a long while, the Philippine Delegation—composed of government, private sector, and civil society—developed country positions on the most important issues. However, the lack of an "Internet governance" mechanism within ICTO stymied the momentum from WCIT, and IG discourse remained underdeveloped in ICTO. See
"ICTO: PH Didn't Sign ITU Treaty As It Might Affect BPO Industry," *Newsbytes Philippines,*17 December 2012, http://newsbytes.ph/2012/12/17/icto-ph-didnt-sign-itu-treaty-as-it-might-affect-bpo-industry/.
[77] See, for example, David Dizon, "Facebook Use in Gov't Saps Productivity: CSC," *ABC–CBN News,* 3 June 2011, http://news.abs-cbn.com/-depth/06/03/11/facebook-use-govt-saps-productivity-csc.
[78] The Supreme Court eventually stuck down many provisions in the Cybercrime Act, including provisions on unsolicited commercial communications, real-time collection of traffic data, and blocking access to computer sites found in violation of the act, but it upheld the provision that allowed the filing of cases against online "libel." See Edu Punay, "Internet libel in cyber crime law unconstitutional" *Philippine Star,* 19 February 2014, http://www.philstar.com/headlines/2014/02/19/1292003/internet-libel-cyber-crime-law-constitutional; and "Supreme Court Declares Cybercrime Law Unconstitutional," Ifex Center for Media Freedom and Responsibility, 20 February 2014, https://www.ifex.org/philippines/2014/02/20/libel_clause/.
[79] "Full Text: Cybercrime Law Constitutional—Supreme Court," *Rappler,* 24 February 2014, http://www.rappler.com/nation/special-coverage/cybercrime-law/51197-full-text-supreme-court-decision-cybercrime-law.

months later.[80] The children's parents contended that the photos had been obtained in violation of the children's privacy rights. The Supreme Court ruled that because the photos were seen by other school students, and then by a teacher, that there was no relevant privacy protection. This was widely criticized for conflicting with the testimony of the students themselves, who said that the photos were viewable only among themselves.[81]

In both cases, debates continued even after the Supreme Court rulings. Tensions in policy development continue to play out because we live in a time where "ubiquitous computing," "big data and analytics," "Internet-of-things"/"Internet of everything," and "smart technologies" are stretching the boundaries of privacy, freedoms of information and expression, information security, commercial transactions, and the local Internet governance ecosystem.

International Treaties

There are a number of key legislative instruments that affect the current Internet governance landscape. The Philippines has signed and ratified the following key international treaties: the International Covenant on Economic, Social and Cultural Rights (ICESCR); International Covenant on Civil and Political Rights (ICCPR); Optional Protocol (OP) to the ICCPR; International Convention on the Elimination of All Forms of Discrimination against Women (CEDAW); OP-CEDAW; Convention on the Rights of the Child; Convention on the Protection of the Rights of All Migrant Workers and Members of their Families; Convention Against Torture; and UN Convention Against Transnational Organized Crime.

Domestic Laws

The domestic laws that currently have an impact on local Internet governance include the following:

Electronic Commerce Act

In the aftermath of the "I Love You" virus incident,[82] the government responded with the Electronic Commerce Act (Republic Act No. 8792), which was enacted on 14 June 2000. Designed primarily to promote e-commerce in the country, a substantial portion of the law was dedicated to enabling the admissibility of electronic documents in court cases. This act eventually led to the development of the Rules on Electronic Evidence spearheaded by the Supreme Court.[83] The law outlines, for the very first time in Philippine history, provisions on hacking, viruses, and online copyright violations. The first Filipino to be convicted of a cybercrime is thought to have been charged under this law. J.J. Maria Giner was prosecuted for the crime of hacking and convicted in September 2005. He admitted to the charge of hacking the government portal "gov.ph" and various other government websites. Sentenced to one to two years of imprisonment and fined PhP 100,000 (approximately USD 1,800), he applied for and was granted probation by the court.

[80]Supreme Court decision, Vivares and Suzara vs. St. Theresa's College, GR No. 202666. See also Jee Y. Geronimo, "SC: STC Did Not Violate Students' Right to Privacy," *Rappler*, 23 October 2014, http://www.rappler.com/nation/72912-sc-decision-stc-students-privacy-rights; and Lira Dalangin-Fernandez, "End of Internet Freedom? Concern Expressed Over SC Decision on Cebu Co-eds, Privacy, Facebook Photos," *InterAksyon*, 27 October 2014, http://www.interaksyon.com/article/98019/end-of-Internet-freedom-concern-expressed-over-sc-decision-on-cebu-co-eds-privacy-facebook-photos.

[81] Geronimo, "SC: STC Did Not Violate Students' Right to Privacy."

[82] The "I Love You" virus case was the first high-profile cybercrime incident in the Philippines. The virus was created and released in 2000 by Onel de Guzman, a computer-programming student, who facilitated its spread through an email which had for its subject an innocuous "I Love You" heading. The virus reportedly caused as much as $10 billion in losses in as many as twenty countries.

[83] Administrative Matter No. 01-7-01-SC. RE: Rules on Electronic Evidence.

Anti-Photo and Video Voyeurism Act

Also known as the Republic Act No. 9995, the Anti-Photo and Voyeurism Act of 2009 prohibits taking photos or videos of a person performing a sexual act. It also prohibits taking an image of a person's "private area," without the consent of that person and under circumstances where there is a reasonable expectation of privacy.[84] Copying or reproducing such photos or videos,[85] selling and distributing,[86] as well as the publishing and broadcasting thereof,[87] are similarly prohibited. Consent given for taking videos or photos is not considered a defence for the subsequent *unauthorized* reproduction, distribution, or publication of such photos or videos. Any record, photo, or video resulting from any of the prohibited acts listed under the law are inadmissible as evidence in any investigation, hearing, or court proceeding.[88]

Anti-wiretapping Law

As far as a regulatory framework on communication surveillance is concerned, the Philippines has a very loose one, beginning with the country's anti-wiretapping law (Republic Act No. 4200) that dates back to 1965. It prohibits the unlawful interception and/or recording through wire or cable tapping of any private communication or spoken word with the use of any recording or surveillance equipment.[89] The possession of any record of such private communication is also deemed unlawful. However, interception and/or recording may be allowed for purposes of gathering evidence in a civil or criminal investigation or trial, provided that the law enforcement officer is authorized by a court order to carry it out.

Human Security Act

In 2007, the Human Security Act (RA 9372) slightly modified the wiretapping law by allowing the surveillance of terrorism suspects, as well as the interception and recording of communications "between members of a judicially declared and outlawed terrorist organization, association, or group of persons or of any person charged with or suspected of the crime of terrorism or conspiracy to commit terrorism" upon a written order of the appellate court.[90] Nevertheless, it maintains the prohibition of surveillance committed against lawyers and clients, doctors and patients, journalists and their sources, and confidential business correspondence.[91]

Anti-Child Pornography Act

The Anti-Child Pornography Act (Republic Act No. 9775) came out in 2009, guaranteeing the fundamental rights of a child against all forms of exploitation and abuse. It is a direct manifestation of the country's compliance with international treaties that concern the rights of children. The law features specific provisions for the effective facilitation of communications surveillance by ISPs. The law requires ISPs, under threat of penalty, to: (1) notify authorities of circumstances indicating that child pornography activities are using its server, (2) preserve evidence of the same, (3) furnish authorities with information regarding users who accessed or attempted to access sites containing child pornography, and (4) install software to ensure that access to or transmittal of child pornography will be blocked or filtered.[92] However, the law maintains that nothing in it may be construed as requiring an ISP to

[84] Sec. 4(a), RA 9995.
[85] Sec. 4(b), RA 9995.
[86] Sec. 4(c), RA 9995.
[87] Sec. 4(d), RA 9995.
[88] Sec. 7, RA 9995.
[89] Rep. Act No.4200, § 1.
[90] Rep. Act No. 9372, § 7.
[91] Ibid.
[92] Rep. Act No. 9775, § 9.

engage in the monitoring of its customers, or the content of their communication.[93] This qualifier may indicate unresolved policy questions surrounding legal surveillance in the country.

Writ of Habeas Data

In 2008, the Supreme Court issued the Rule on the Writ of Habeas Data.[94] The writ is a remedy available to individuals whose right to privacy in life, liberty, or security is violated or threatened by the unlawful act of another individual or entity engaged in the gathering or storage of information pertaining to them (e.g., his or her person, family, home, and/or correspondence).[95] Thus, it allows people to determine what information is being collected about them, whether by law enforcement agencies or private entities, including the purpose or use of such collection. If successful, a petitioner may ask for the updating, rectification, suppression, or destruction of the database or information being kept about him/her, and, where threats are present, seek an order prohibiting the act complained of.[96]

Data Privacy Act

Another legal reference for communications surveillance is the Data Privacy Act of 2012 (RA 10173), which protects individual personal information in information and communications systems in the government and the private sector. The scope of the law includes all types of privileged communication.[97] It also modifies or amends the Human Security Act, insofar as the provision on communications surveillance is concerned.[98] The act regulates the processing of an individual's personal information that is collected by both public and private entities.[99] It is modelled after the European Union's Data Protection Directive, which was adopted in 1995.[100] The law calls for the establishment of the National Privacy Commission (NPC), headed by a privacy commissioner and two deputy privacy commissioners. One of the commission's tasks is to draft the act's implementing rules and regulations. In March 2016, more than three years after the law was passed, the National Privacy Commission was finally appointed.[101]

Cybercrime Prevention Act

The Cybercrime Prevention Act (Republic Act 10175) became law only one month after the Data Privacy Act, approved on 12 September 2012.[102] It stipulates different cybercrime offences and corresponding penalties. In terms of regulating communication surveillance, the law, as enacted, authorized law-enforcement authorities, with the required assistance of service providers, to collect or record real-time traffic data[103] on communications made through a computer system.[104] Other data to be collected requires a court warrant.[105] The law also provides for a mandatory data-retention regime. Traffic data, subscriber information, and content data from service providers were to be preserved for a minimum of six months, with law-enforcement authorities able to order a one-time six-month

[93] Ibid.
[94] Supreme Court Administrative Matter No. 08-1-16-SC.
[95] SC Admin. Matter No. 08-1-16-SC, § 1.
[96] SC Admin. Matter No. 08-1-16-SC, § 6.
[97] Rep. Act No. 10173, § 3(k).
[98] Sec. 44. *Repealing Clause.* The provision of section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007," is hereby amended. Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.
[99] Republic Act No. 10173, 15 August 2012, http://www.gov.ph/2012/08/15/republic-act-no-10173/.
[100] Kim Luces, "How the Data Privacy Act Impacts PHL Businesses," *GMA News Online*, 11 October 2013, http://www.gmanetwork.com/news/story/330365/scitech/technology/how-the-data-privacy-act-impacts-phl-businesses.
[101] See "DOST Exec Named First Commissioner of National Privacy Commission," *Newsbytes Philippines*, 7 March 2016, http://newsbytes.ph/2016/03/07/dost-exec-named-first-commissioner-of-national-privacy-commission/.
[102] *Republic Act No. 10175*, 12 September 2012, http://www.gov.ph/2012/09/12/republic-act-no-10175/.
[103] This refers only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities. Sec. 12, RA 10175.
[104] Rep. Act No. 10175, § 12.
[105] Ibid.

extension if data are to be used as evidence. Service providers are also mandated to keep the preservation order and compliance confidential.

The implementation of the *Cybercrime Prevention Act* was delayed—first under a 120-day temporary restraining order, followed by an indefinite hold—after the Supreme Court received fifteen petitions questioning the constitutionality of some of its provisions, including the penalties for libel, and the provisions that make it easier for authorities to spy on citizens using electronic media.[106]

The petitions called for the Supreme Court (SC) to strike down provisions contained in sections 4, 5, 6, 7, 12, and 19. Sections 4 and 5 cover various offences, including online libel, while sections 6 and 7 impose a higher degree of punishment for those found guilty of libel, yet also allowing them to be charged under the revised penal code for the same offence.[107] Also known as "double jeopardy," the revised penal code violates article 3, section 21 of the constitution, which states that "no person shall be twice put in jeopardy of punishment for the same offense."[108] Moreover, the petitioners criticized section 12 on the real-time collection of traffic data, and section 19, which authorizes the DOJ to restrict or block access to data deemed to be in violation of the law.[109] In 2014, the SC ruled that the online libel provision is constitutional, though it struck down other provisions, including sections 12 and 19. It also clarified that only the original author of libelous material can be penalized, and not those who merely received or reacted to it.[110]

Citizens took to social media to criticize the bill, which they saw as infringing on their freedom of expression. Hackers also defaced government and private websites in protest. The front pages of the websites of the *Bangko Sentral ng Pilipinas* (Central Bank) and the Metropolitan Waterworks and Sewerage System were replaced with black screens showing a written message from a group who called itself Anonymous Philippines.[111]

In August 2015, the law's implementing rules and regulations were issued by the Department of Science and Technology (DOST), the DOJ, and the Department of the Interior and Local Government (DILG). In a surprising turn of events, the rules now explicitly provide for the collection of computer data, which consist of both content and traffic data. Given that they seem to have brought back a provision already struck down by the Supreme Court, the rules as presently written appear to be susceptible to another constitutional challenge, and may suffer the same fate as their parent statute. It would seem that its authors also expanded its scope, and interpreted it in a way that amends the country's anti-wiretapping law and adopted treaty provisions, without going through the appropriate legal process.

There are also a number of policy proposals currently pending before the country's legislature that are worth mentioning. In response to the controversial anti-cybercrime law, the Magna Carta for Philippine Internet Freedom (MCPIF)[112]—a crowd-sourced Internet law bill—was filed as House Bill No. 1086 by Rep. Kimi Cojuangco and as Senate Bill No. 53 by Senator Miriam Defensor-Santiago. The bill guarantees a number of basic rights, such as the right to free expression, right to privacy, and right to access.[113] If passed, the MCPIF

[106] Mark Merueñas, "Internet Libel in Cybercrime Law Constitutional – SC," *GMA News*, 18 February 2014, http://www.gmanetwork.com/news/story/348945/scitech/technology/internet-libel-in-cybercrime-law-constitutional-sc.
[107] Ibid.
[108] *1987 Constitution*, article 3, Approved 2 February 1987, http://www.comelec.gov.ph/?r=References/RelatedLaws/Constitution/1987Constitution/Article3.
[109] Phoebe Magdirila, "Philippines' Cybercrime Law Now in Effect, Punishing Online Libel Is Constitutional," *Tech in Asia*, 18 February 2014, https://www.techinasia.com/philippines-cybercrime-law-effect-punishing-online-libel-constitutional/.
[110] "Full Text: Cybercrime Law Constitutional."
[111] Kim Arveen Patria, "Gov't Websites Hacked in Anti-cybercrime Law Protest," *Yahoo News*, 26 September 2012, https://sg.news.yahoo.com/gov-t-websites-hacked-in-anti-cybercrime-law-protest.html?page=all.
[112] "Full Text of the Magna Carta for Philippine Internet Freedom (MCPIF)," Democracy.net, http://democracy.net.ph/full-text/.
[113] Jillian York, "A Brief Analysis of the Magna Carta for Philippine Internet Freedom," Electronic Frontier Foundation, 8 July 2013, https://www.eff.org/deeplinks/2013/07/brief-analysis-magna-carta-philippine-internet-freedom.

would repeal the Cybercrime Protection Act. To date, however, it has continued to languish at the lower house's committee level.[114]

In 2015, House Bill No. 5231, otherwise known as "An Act Requiring the Registration of All Users of Prepaid Subscriber Identity Module (SIM) Cards," was approved by the House of Representatives. It aims to prevent the use of mobile phones in illegal activities by addressing the current fact that anyone can buy prepaid SIM cards at any store without providing identification. The bill requires buyers to fill out and submit a registration form to the vendor, together with identification. The documents are forwarded to the mobile phone service provider who, in turn, furnishes the NTC with copies.[115] According to the bill's proponent, data gathered from the forms should be available to law enforcers when needed.[116] This is despite there being no clear process and guidelines yet on the storage and retrieval of data. Similar proposals for mandatory SIM card registration have been filed in the Seventeenth Congress.[117]

NATIONAL POLICY INSTITUTIONS

ICTO and Its Predecessors

For many years, the government has resisted creating a cabinet-level ICT agency, describing it as an "unnecessary bureaucracy."[118] In June 2015, however, the senate approved Bill No. 2686, which seeks to establish a Department of Information and Communications Technology (DICT).[119] In October 2015, the House of Representatives approved its counterpart proposal (House Bill No. 6198).[120] Its proposed functions include, among other things, coordinating with the NTC, the NPC, and the Cybercrime Investigation and Coordination Center (CICC)—an agency created as a result of the anti-cybercrime law. On 23 May 2016, the DICT bill was finally signed into law by President Aquino.[121]

The Philippines has not been entirely without ICT regulators. In the 1980s, the Philippines created the IT Coordinating Council (ITCC) as the first body to coordinate the formulation and implementation of ICT policies. It eventually became the National IT Council (NITC) in the 1990s, which then merged with the E-commerce Promotion Council and became the IT and E-commerce Council (ITECC).[122] The ITECC was abolished in 2004 when a new governmental body—Commission on Information and Communications Technology (CICT)—was formed to implement the government's ICT agenda.[123] The CICT was dissolved in

[114] "Miriam Laments Senate Inaction on Bills vs. 'Epal' Politicians, Political Dynasties," *GMA News Online,* 19 June 2015, http://www.gmanetwork.com/news/story/506974/news/nation/miriam-laments-senate-inaction-on-bills-vs-epal-politicians-political-dynasties.
[115] Jess Diaz, *"House OKs* Bill *on* Registration *of* Prepaid SIM Cards," *The Philippine Star* 23 May 2015, http://www.philstar.com/headlines/2015/05/23/1457797/house-oks-bill-registration-prepaid-sim-cards.
[116] Ryan Chua, "Telcos Oppose Prepaid SIM Card Registration," *ABS–CBN News,* 11 August 2015, http://www.abs-cbnnews.com/business/08/11/15/telcos-oppose-prepaid-sim-card-registration.
[117] Senate Bill Nos. 7, 105, 203, 252, and 1160.
[118] J.M. Tuazon, "Myanmar Leaps Ahead of the Philippines in Creation of ICT Ministry," *InterAksyon*, 16 November 2012, http://www.interaksyon.com/infotech/myanmar-leaps-ahead-of-the-philippines-in-creation-of-ict-ministry.
[119] Yuji Vincent Gonzales, "Senate OKs Bill Creating ICT Department," *Inquirer.net,*2 June 2015, http://newsinfo.inquirer.net/695652/senate-oks-bill-creating-ict-department.
[120] Paolo Romero, "House OKs Creation of ICT Department," *The Philippine Star*, 12 October 2015, http://www.philstar.com/headlines/2015/10/12/1509809/house-oks-creation-ict-department.
[121] "Aquino Signs Law Creating DICT, Restructuring DOTC," *Rappler,* 23 May 2016, http://www.rappler.com/nation/133992-aquino-signs-law-ict-department.
[122] David Dizon, "Reforms in IT Sector Urged to Advance RP Competitiveness,"*ABS–CBN News,* 11 April 2008, http://www.abs-cbnnews.com/nation/04/11/08/reforms-it-sector-urged-advance-rp-competitiveness-0.
[123] Ibid.

2011 when President Benigno Aquino III reorganized and renamed the agency ICTO, and placed it under the DOST's purview.[124]

When ICTO was created, it absorbed the functions of the National Computer Center, the Telecommunications Office of the DOTC, and the CICT.[125] It assumed the role as the government's main ICT policy development agency and lead implementer of key e-government initiatives. Aside from normal transition issues, a more strategic "rationalization plan" was devised to unify disparate agencies and streamline their overlapping functions.

Today, the NTC remains the legacy regulatory agency for local telecommunications, and continues to exist as a separate quasi-judicial body under the Office of the President. It is mandated to perform crucial policy-related functions inherent to its formal role. However, it also continues to be subjected to criticisms because of its weak enforcement capacity, its politicized nature (e.g., NTC commissioners are political appointees with no fixed terms), and allegations of regulatory capture (e.g., from problematic VOIP guidelines to lack of consumer protection against poor Internet service).

Anti-Cybercrime Groups

The Cybercrime Investigation and Coordination Center

The Cybercrime Investigation and Coordination Center (CICC) was created pursuant to the Cybercrime Prevention Act in 2012. The CICC is chaired by the executive director of ICTO, and vice-chaired by the director of the National Bureau of Investigation (NBI).[126] Members of the CICC include the chief of the Philippine National Police (PNP), the head of the DOJ's Office of Cybercrime, and one representative each from the private sector and academia. Among CICC's tasks are formulating a national cybersecurity plan and providing assistance in responding to cybercrime offences through a computer emergency response team (CERT).[127]

PNP Anti-Cybercrime Group

With an increase in the incidence of cybercrimes,[128] the PNP has also established the Anti-Cybercrime Group as the primary unit responsible for implementing the cybercrimes law and launching anti-cybercrime campaigns on behalf of the police and national government.[129] On 17 September 2015, President Aquino III created the National Cybersecurity Inter-Agency Committee through Executive Order No. 189. Operating under the Office of the President, the unit is charged with coordinating government agencies and other relevant sectors in the preparation of appropriate effective measures to strengthen their cybersecurity capabilities against existing and future cyber threats. It is chaired by the executive secretary, and is co-chaired by both the director general of the National Security Council (NSC) and the secretary of the DOST.[130]

[124] J.M. Tuazon, "Aquino Dissolves ICT Commission," *GMA News*, 30 June 2011, http://www.gmanetwork.com/news/story/224874/scitech/aquino-dissolves-ict-commission.
[125] ICTO was created by Executive Order No. 47. See details at http://www.gov.ph/2011/06/23/executive-order-no-47-s-2011.
[126] "Cybercrime body to convene in October," Republic of the Philippines Department of Information and Communications Technology, http://www.dict.gov.ph/cybercrime-body-to-convene-in-october/.
[127] Ibid.
[128] Julliane Love de Jesus, "Number of Cybercrime Cases Surged in Last Two Years—PNP-ACG," *Inquirer*, 27 August 2015, http://technology.inquirer.net/44023/number-of-cybercrime-cases-surged-in-last-2-years-pnp-acg.
[129] "PNP ctivates anti-cybercime unit," *GMA News*, 21 March 2013, http://www.gmanetwork.com/news/story/300244/scitech/technology/pnp-activates-anti-cybercrime-unit.
[130] Executive Order No. 189, s. 2015, §8.

Philippine CERTs

As of 2016, the envisioned national CERT has not yet been constituted. Pursuant to the Department of Information and Communications Act of 2015 (RA No. 10844), the mandate of establishing the National CERT (NCERT) is now with the newly formed Department of Information and Communications Technology (DICT), which is still undergoing its own organizational issues inherent to any new national agency. Executive Order No. 189 issued in September 2015 further provides that the NCERT "shall issue guidelines on the handling of government data/information by members of CERTs to be organized within the respective agencies and shall perform oversight and audit functions as to compliance with said guidelines."

The only CERT that had existed in the country was the private-sector-led Philippine Computer Emergency Response Team (PhCERT). Organized some fifteen years ago, PhCERT is registered as a nonstock, nonprofit organization. Its members are certified information security professionals and practitioners who serve on a purely voluntary basis. It conducts awareness programs for its members and other organizations and has participated in various public- and private-sector technical working groups and committees on matters relating to information security, ICT legislation, and rules development. PhCERT claims to be a founding member of the Asia-Pacific CERT (APCERT) organized some twelve years ago which conducts annual conferences within the Asia-Pacific Region, but admits to being inactive during the past several years.[131]

Limited by its lack of resources and full-time staff, and as a result of its purely private-sector nature, it cannot play the role of the envisioned formal national CERT. It can only provide its members a venue to learn from each other and hone skills in the field of information security, and provide them occasional consultancy opportunities. It is now transitioning to be a coordinating centre in addressing information security incidents, and has assumed a new name: the PH CERT Coordination Center.[132]

National Privacy Commission

The National Privacy Commission, which was created by virtue of the Data Privacy Act of 2012,[133]is tasked with creating and promulgating the implementing rules and regulations of the Data Privacy Act and to issue advisory opinions and propose amendments or modifications on Philippine laws and policies relating to privacy and data protection. In March 2016, shortly before the election ban on appointments commenced, the commissioner and deputy commissioners were finally appointed.[134]

Department of Budget and Management

The push for strategic e-government was enabled by support from the powerful Department of Budget and Management (DBM) which financially supported and fostered innovative inter-agency collaborations behind its key programs, such as the Medium-Term ICT Harmonization Initiative (MITHI). That project herded government agencies toward a more unified ICT enterprise architecture and planning, and the Open Government initiative.[135]

[131] Email and phone interview with PH Cert CERT long-time President Lito Averia, (August 2016).
[132] Philippine Computer Emergency Response Team Coordination Center, http://phcert.cc/.
[133] *Republic Act No.* 10173.
[134] "DOST Exec Named First Commissioner"; "Microsoft PH Exec, Lawyer-Doctor Appointed Deputy Chiefs at Privacy Agency," *Newsbytes Philippines,* 9 March 2016, http://newsbytes.ph/2016/03/09/microsoft-ph-exec-lawyer-doctor-appointed-as-deputy-chiefs-of-privacy-commission/.
[135] The Philippines was a founding member of the Open Government Partnership and the DBM was the lead agency, curiously not the ICTO.

STATE CAPACITY ISSUES, GAPS IN ICT LEADERSHIP

Although the ICTO's creation in 2011 surprised many,[136] there are those who believe that the historical shifts in ICT policy administration through the years should have hinted that another change was forthcoming.[137] The designation of DOST as its supervising authority—a move that has its strengths and weaknesses—was designed to embed ICT development within the scope of science and technology. That its mandate consisted of those previously assigned to three different agencies was more of a strategic decision, and the succeeding "ICTO Rationalization Plan" or RatPlan became an opportunity to reimagine an ICT policy development agency for the twenty-first century.[138]

Unfortunately, the RatPlan was complex and tedious, and took a lot of effort to craft and implement. Streamlining three disparate agencies with more than 3,000 workers to what was seen as an "ideal" single structure of less than a thousand was never going to be an easy feat.[139] Understandably, many of the government workers involved were protective of the old and familiar structures, roles, and functions. The reorganizational effort left the office grossly understaffed and incapable of properly addressing many of the relevant prevailing issues. An important initiative called the Integrated Government Philippines (iGov) Project became the State's de facto e-government flagship project.[140] However, many other ICT policy areas, particularly in "e-society" matters, remained and received little attention and support.

The previous ICT National Plan ("Philippine Digital Strategy" or PDS) adopted by ICTO's predecessor was created, but never fully embraced and fleshed out. The plan identified key actions to ensure that all citizens enjoy the opportunities that the Internet brings.[141] It also related directly to sound Internet governance, including "modernizing ICT policies, laws, and institutions," "ensuring a secure, reliable ICT infrastructure, and safe online experience," as well as sections that present universal access goals. Unfortunately, not even ICTO's establishment was enough to realize the key result areas it envisioned. Important policy outputs such as the National Broadband Policy, National Cloud Computing Policy, and Data Privacy Framework languished, and many e-society measures for universal access, digital literacy, and gender equity in ICTs were left unarticulated. E-business also became much more of an ICT industry promotions arm within ICTO, with no policy development in e-commerce, mobile money, and crypto currency having materialized thus far.

Nevertheless, ICTO's efforts did yield some policies. For one, iGov gave birth to the new eGoverment Master Plan (eGMP). The country's digital TV migration strategy also evolved. The national cybersecurity infrastructure was revitalized, while an open standards framework was developed for government interoperability. Finally, there was the launch of the groundbreaking TV White Space (TVWS) strategy for rural connectivity within an evolving local "micro Telco" framework,[142] followed by the Free Public Wi-Fi initiative that began in 2014.

ICTO also supported selected key legislative initiatives (e.g., a "national ICT policy framework" that was eventually integrated into the draft DICT bill), even as it failed to exert proper guidance for major legislations

[136] ICTO was created by Executive Order No. 47; see http://www.gov.ph/2011/06/23/executive-order-no-47-s-2011.
[137] For a summary of institutional development of ICT policy in the Philippines, see Alegre and Tuano, Global Information Society Watch 2007 Philippine Report, Foundation for Media Alternatives, https://www.giswatch.org/en/country-report/civil-society-participation/philippines.
[138] One of the report's authors had an intimate knowledge of the development and rollout of the ICTO RatPlan as senior consultant in 2012–2013.
[139] See, for example, "Rationalization Hits 1,900 ICTO Workers," *Newsbytes Philippines,* 25 July 2016, http://newsbytes.ph/2013/07/25/rationalization-hits-1900-icto-workers/.
[140] See Integrated Government Philippines project, http://i.gov.ph/.
[141] PDS, Strategic Thrust # 2 Internet Opportunities for All, http://dict.gov.ph/wp-content/uploads/2014/06/philippine-digital-strategy-2011-2015.pdf
[142] See "ICTO lauded for TV White Space Initiative," Republic of the Philippines Department of Information and Communications Technology, http://www.dict.gov.ph/icto-lauded-for-tv-white-space-initiative/.

(e.g., Cybercrime Prevention Act).[143] With respect to some policies, such as the Data Privacy Act, the office provided some support to civil society groups,[144] but stopped short of advocating their implementation. It also did not exert influence or oversight on the NTC's regulatory role, which has been a key gap in aligning policy, implementation, and regulation.

A comprehensive assessment of ICTO cannot be outlined here,[145] but what is clear at this point is that in many areas of ICT policy (e.g., Internet governance), the office had neither the resources nor the inclination to tackle key issues, especially those that emerged from multistakeholder platforms. This gap illustrates the state bureaucracy's low capacity in addressing the challenges of Internet governance and explains the government's lack of participation in fora like the Internet Governance Forum.

Lack of Coordination Between State Agencies

Sections of the government—beyond ICTO and NTC—have thus far failed to align their respective agendas.

As the main ICT policy agency, ICTO is supposed to reach out to different agencies so that the appropriate policies can be formulated. It also needs to forge strategic partnerships with legislators in promoting the necessary legal and regulatory reform. Meanwhile, all other government agencies, especially those that are crucial to ICT development, must also align themselves with ICTO's priorities. Thus far, this has not always been possible for a variety of reasons.

To be sure, ICTO has had some groundbreaking partnership with the Department of Budget and Management,[146] which supported the ICTO's rationalization and its eventual role as the government's chief technology office (if not its chief information office). Their relationship brought much-needed resources previously unavailable for e-government projects. ICTO also managed to maintain a close interagency cooperative arrangement in the area of national cybersecurity. While some strategic gaps are apparent, ICTO's new structure provided for a permanent national coordinator for cybersecurity with a rank of assistant secretary.

It is in its relationship with those institutions more closely affiliated with Internet and human rights, in general, that ICTO needs to improve. Civil society actors have regularly pointed to ICTO's inability to coordinate with other sectoral agencies to develop domain-specific ICT policy areas. In particular, these sectoral agencies include:

- The Commission on Human Rights (CHR), which needs to appreciate how the online environment is also a site for human rights violations;
- The Philippine Commission on Women (PCW), which is in charge of gender rights advocacy within the country, where gender-related online violence is on the rise.
- ICTO did conduct occasional joint activities with the National Commission on Disability Affairs (NCDA). However, these activities were limited to job fairs for persons with disabilities (PWDs), and were without a programmatic investigation of the exclusion of PWDs in national ICT discourses, as well as in developing appropriate accessibility tools.

Lack of Coordination in Legislative Development

[143] *Republic Act (RA) 10175* was immediately challenged in the Supreme Court for its overly broad reach and concerns about its effects on online free expression and digital privacy.
[144] RA 10173, the Data Privacy Act of 2012.
[145] FMA is starting an initiative on assessing ICTO's performance (2012–2016) and crafting recommendations for the next administration.
[146] DBM Undersecretary Richard Moya was a visionary leader in ICT governance who worked well with ICTO.

Civil society organizations (CSOs) have also noted breakdowns in coordination in relation to some key legislative areas:

- The Cybercrime Prevention Act. Not only was ICTO unable to vet the draft bill properly, but subsequent analyses by its own consultants were also critical of the law.[147]
- The Department of Information and Communications Technology Act. The push for the ICT department's creation was contested within the ICTO leadership, who once believed that President Benigno Aquino III had little to no support for the bill. Eventually, however, they supported and helped draft the 2014 Senate bill.[148]
- Data Privacy Act. ICTO failed to push for a speedy implementation of the law, which has been in force since 2012.
- ICTO did not nurture enough champions in Congress to push for needed legislative reform (e.g., NTC reorganization, updating of the Telecommunications Act). Its gaps in policy development were readily apparent, given the lack of senior personnel who had both the time and expertise to deal with many of the prevailing issues.

Some see the establishment of the DICT as a solution to this lack of coordination. Such disjointed efforts are presumed to stem from ICTO's lack of stature since it is merely an attached agency to DOST. Others try to explain how the lack of unified national purpose point to the absence of a strategic ICT policy agenda that can unite all stakeholders.[149] Some type of national roadmap could serve as a common agenda to focus efforts collectively.

Lack of Multistakeholder Policy Development Spaces

In global discussions of ICT policy, many have held up the multistakeholder model of governance as ideal for managing a public commons such as the global Internet. Since the landmark World Summit on the Information Society (WSIS) in 2003 and 2005, and in a number of spaces such as WSIS's successor—the Internet Governance Forum (IGF), held under the auspices of the United Nations,[150] there have been more voices advocating for moving away from purely multilateral (i.e., intergovernmental models) to more inclusive ones that include non-state actors (i.e., NGOs, private sector, academia, and the technical community).[151]

1. ICTO and the Rise and Fall of NICTAC

Although ICTO has attempted to engage different stakeholders in the past, these efforts have neither been consistent nor programmatic. ICTO regularly invites nongovernment stakeholders to its events and consultations, but has not, to date, established formal mechanisms to institutionalize such a consultative approach.

[147] ICTO insiders admitted to such, as attested to by Winthrop Yu, president of ISOC Philippines, who personally met with ICTO staff and consultants on the cybercrime law. Interview with Mr. Yu, October 2015.
[148] See the editorial "State of ICT," *Visayan Daily Star*, 13 October 2015, http://visayandailystar.com/2015/October/13/opinion.htm. Legislators who passed the bill have urged the president not to veto their legislative action http://2016.mb.com.ph/2016/01/21/solon-urges-aquino-not-to-veto-bill-separating-dotc/.
[149] Interview with Dr. Emmanuel Lallana of Ideacorp, November 2015.
[150] See the Internet Governance Forum website at www.intgovforum.org.
[151] See "Multistakeholder Model," http://icannwiki.com/Multistakeholder_Model. Also Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum* (Canberra: Terminus Press, 2008). Chapter 4 of the book contains descriptions, strengths, and weaknesses of specific governance models.

A laudable but short-lived attempt was launched in 2013. With the prodding and assistance of CSOs and ICT-sector organizations, and in keeping with the spirit of the previous Philippine Digital Strategy (PDS) processes that resulted from broad multistakeholder consultations, ICTO agreed to organize a platform called the National ICT Advisory Council (NICTAC). This effort received support from a broad swath of nongovernmental actors who were serious about leveraging their respective strengths in support of ICTO in key policy areas. NICTAC was launched in October 2013, and multisectoral study groups were established for certain priority areas: cyber security, the national broadband plan, cloud computing, data privacy, public finance and ICT procurement, ICT education, and a code of ICT laws.[152] The understanding then was that new working groups could be added when the situation called for it. Initial meetings by these groups yielded some specific proposals, particularly in data privacy and cyber security. However, budgetary support faltered, and ICTO did not provide the necessary leadership to keep the initiative going. By mid-2014, NICTAC became dormant.

Since then, nothing close to NICTAC has been convened again. While ICTO continues to call the occasional public forum (e.g., the recent consultation on the long-delayed broadband plan, as well as one on developing a new PDS), many CSOs felt that these were half-hearted attempts to rush more accomplishments before the 2016 elections, rather than part of an overall strategy of multistakeholder engagement.

2. NTC and Regulatory Challenges

The NTC, for its part, has also conducted public consultations. It conducts them regularly through open public hearings before they issue guidelines or memorandum circulars. In such venues, big businesses, civil society, academics, and even the public at large are open to talk and share their insights on various topics. Asked about the role these consultations play in their policy-making processes, newly appointed Deputy Commissioner Edgardo Cabarios noted that, "consumer groups and civil society are highly valued stakeholders as they are the ones advocating for transparency and reforms."[153]

However, these public processes can sometimes mask the strength of powerful lobbies such as large telecommunications companies who do not hesitate to deploy their vast financial and legal resources to stymie any ruling that favours consumers. In fact, a number of legal cases filed by telcos questioning even minor NTC rulings are languishing in the courts today. In 2010, a landmark "Significant Market Power" antimonopoly framework based on extensive research was about to be issued by the NTC, before it was "withdrawn" after the biggest telco opposed it. With researchers and industry analysts routinely referring to the NTC as a "captured" regulator,[154] civil society groups have thrown their support behind a bill reorganizing the agency.[155]

3. International Engagement: Multilateral over Multistakeholder?

One of the roles of ICT policy-makers is to engage with regional or international counterparts in building knowledge, skills, and capacity. ICTO and NTC remain active in traditional institutions like

[152] "ICT Advisory Council Convenes Study Groups," Republic of the Philippines Department of Information and Communications Technology, http://www.dict.gov.ph/ict-advisory-council-convenes-study-groups/.
[153] Interview with Dir. Edgardo Cabarios of NTC, October 2015.
[154] See, for example, Rafaelita Aldaba, "Opening Up the Philippine Telecommunications Industry to Competition," Case Study World Bank Institute, May 2000, http://regulationbodyofknowledge.org/wp-content/uploads/2013/03/Aldaba_Opening_Up_the.pdf.
[155] The proposed NTC reorganization bills include, among other provisions, fixed terms for appointed commissioners (many of whom are pressured to resign at the first sign of "autonomy"), and fiscal autonomy for the commission through the retention of spectrum users fees—important to raise salaries of personnel, which remain low (making them prone to corruption).

the International Telecommunications Union (ITU) and its Asian regional structure (Asia Pacific Telecommunity). They are also very active in other intergovernmental dialogues that tackle Internet governance issues but they are considered less inclusive of other parties outside of governments from their processes. Aside from ITU conferences,[156] the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), and the Association for Southeast Asian Nations Telecommunications and Information Ministers (ASEAN TELMIN)—both important intergovernmental ministerial meetings—regularly see Philippine delegates in their events.

However, the same enthusiasm is noticeably absent when it comes to other international Internet governance spaces that are more inclusive to nonstate actors. They include the Internet Governance Forum (IGF)—the most dynamic post-WSIS multistakeholder space for governments, private-sector representatives, and civil society to date—which regularly convenes to discuss and debate significant issues in a cross cutting way. The IGF has gained prominence and even cascaded into regional (i.e., Asia Pacific Regional IGF) and national iterations (many countries now convene their own national IGFs).

For the past several years, the Philippines has not sent any official representative to the annual IGF meetings. Its failure to engage with the forum in any significant way has resulted in its inability to keep up with the evolving policy landscape abroad.[157]

The country has also rarely sent representatives to meetings of the Internet Corporation for the Assignment of Names and Numbers (ICANN) (the venue of much strategic discussion about the future of the Internet names and numbers space). Although in many ways NICTAC drew on the multistakeholder model of the Internet Engineering Task Force (IETF)—another inclusive standards body that became the template of NICTAC's "working groups"—its demise does not speak well of the government's resolve to pursue a multistakeholder policy development track.

Civil society groups view the ICTO's lack of involvement in multistakeholder processes as having a detrimental effect on the quality and efficacy of national ICT policy development. The Philippines will not be able to keep up with many of the important ICT policy issues regularly being discussed in important multistakeholder platforms if it continues to ignore them or refuse to attend their gatherings. Indeed, many consider the IGF and ICANN to be at the cutting edge of Internet governance discussions so by not participating in these processes the Philippines is a laggard in this regard.

Civil Society Engagement

Outside of the government and private sector, civil society engagement in Internet-related issues in the Philippines remains low. In the wake of the public outcry surrounding the passage of the controversial cybercrime law, the Foundation for Media Alternatives (FMA) convened the Philippine Internet Freedom Alliance (PIFA), a coalition of organizations and individuals opposed to the implementation of the legislation. In recent years, however, organizations like the Computer Professionals Union (CPU) and Democracy.Net have also ramped up their work in this area, with Democracy.Net spearheading the drafting process of a proposed Magna Carta for Philippine Internet Freedom. They are now joined by the local chapter of Internet Society (ISOC PH), and a growing number of organizations for programmers and game developers, as well as

[156] ITU has "sector members" composed of the big national telcos/carriers. In response to long-standing criticism it has recently opened up membership to civil society organizations. As a UN agency, it remains at its core an intergovernmental body.
[157] Jake Soriano, "PH Gov't officials absent in global Internet Governance Forum [VERA Files]," 6 September 2014, https://sg.news.yahoo.com/blogs/the-inbox/ph-govt-officials-absent-in-global-internet-governance-043904420.html.

consumer groups and individual advocates. Collectively, however, their voice has yet to reach a level of significance that is enough to challenge the stranglehold by big businesses and, to some extent, the government, on Internet discourse in the country.

For the past several years, there have been efforts to organize events aimed at encouraging meaningful multistakeholder dialogue on relevant ICT-related issues. They include instances where civil society organizations like FMA, PIFA, and ISOC PH have maximized the use of existing platforms (e.g., NTC public hearings, NICTAC in 2013–14, partnerships with ICTO on popularizing the Data Privacy Act 2012–2014, legislative hearings in the senate and lower house), or have carved out new ones to raise public interest on various ICT issues.

In so doing, they have come to work with other CSOs and human rights defenders like the Philippine Alliance of Human Rights Advocates (PAHRA) to hold various events, such as the first-ever Philippine Multistakeholder Forum on Internet Governance in March 2015.[158] The forum was part of the pre-event activities of RightsCon Southeast Asia 2015, which FMA co-organized and hosted in Manila. It was well attended by government officials, the private sector, and technical organizations from all over the country. It was followed by a pre-IGF Brazil consultation held on 21 October 2015 by ICTO in partnership with ISOC PH and FMA, which was intended as a preparatory forum for the government's planned participation in the 2015 IGF in Brazil.[159] Despite this, ICTO still failed to attend the IGF.

The Philippines has never convened a domestic edition of the IGF, or any counterpart forum. Despite years of lobbying for some sort of national IGF process, ICTO has not invested in a similar platform—unlike its progenitor, which regularly convened "ICT summits" with the private sector and civil society. Unsurprisingly, this has disappointed many CSO actors. FMA and ISOC PH, in particular, view the regular multistakeholder Internet governance events as having the potential to evolve into a national IGF, if only support was forthcoming from the Philippine government.

Both traditional and social media have also played a key role in stimulating the interest of the general public and government officials in further examining how the poorly regulated Internet is dominated by private corporations. Popular campaigns against the early version of the cybercrime law were effective in illustrating how "online martial law" could compromise freedom of expression and privacy rights.[160] Meanwhile, FMA and the Association for Progressive Communications' (APC) efforts in mapping local online violence against women also help popularize the "invisible" side of VAW.[161]

BOX 2. The Philippine Declaration on Internet Rights and Principles[162]

On 4 November 2015, civil society and ICT policy communities achieved a milestone in the form of the Philippine Declaration on Internet Rights and Principles, launched

[158] See "The Future of #PH Internet: A Multistakeholder Forum on Internet Governance, Human Rights, and Development," http://104.236.169.13/FMA/?p=278.
[159] "PH Internet Stakeholders Prepare for the United Nations Global Internet Governance Forum in Brazil," Republic of the Philippines Department of Information and Communication Technology, http://www.dict.gov.ph/ph-internet-stakeholders-prepare-for-the-united-nations-global-internet-governance-forum-in-brazil/.
[160] See "Activists say No to 'Cyber Martial Law.'" Global Voices Advocacy, 11 February 2014, https://advox.globalvoices.org/2014/02/11/february-11-activists-say-no-to-cyber-martial-law-digital-surveillance-in-philippines/.
[161] See "Sixteen Days of Activism Against Gender-based Violence," Take Back the Tech, https://www.takebackthetech.net/.
[162] See http://Internetrightsdeclaration.fma.ph/about/.

after several months of collective drafting and consultations with various civil society, technical groups, and other experts.[163]

The initiative was launched during the Philippine Multistakeholder Forum on Internet Governance, Human Rights, and Development organized by FMA on 23 March 2015. It was inspired by many other similar initiatives of a global or national (e.g., Brazil, Italy) scope. A drafting team, consisting of individuals from diverse backgrounds, developed the declaration's content. There were broad consultations held in Metro Manila, Davao City, and Cebu City from August to October 2015 to solicit inputs on the initial draft. The content of the declaration was also made available online for the inputs and suggestions of others who could not join the face-to-face consultations.

The declaration focused on ten areas: (1) Internet access for all; (2) democratizing the architecture of the Internet; (3) freedom of expression and association; (4) right to privacy and protection of personal data; (5) gender equality; (6) openness and access to information, knowledge, and culture; (7) socio-economic empowerment and innovation; (8) education and digital literacy; (9) liberty, safety, and security on the Internet; and (10) Internet and ICTs for environmental sustainability. The declaration is a reflection of the dreams, hopes, and aspirations of Filipinos for what the Philippine Internet should be. It hopes to serve as the basis for public education, advocacy, networking, and campaigns on ICT, human rights, and development.

By year's end, twenty-three organizations had signed the declaration with many more organizations expressing interest.

Content Controls

In the Philippines, Internet content is considered media, not unlike its more traditional peers: print, radio, and TV. This designation is significant considering that the country's press is largely regarded as free, with a mixture of self-regulation and traditional legal boundaries (e.g., against libel or "obscenity"). Compared to its Southeast Asian neighbours, the Philippines does not have an extensive history of imposing controls on online content.[164] Nevertheless, recent developments suggest that content controls could be on the horizon.

Prior to 2013, there was no evidence of state-level web filtering on Internet Service Providers (ISPs) in the Philippines. Research conducted by the OpenNet Initiative (ONI) tested for web filtering in the country during two periods: in 2006,[165] 2007–2008,[166] and 2009–2010.[167] This research did not identify any instances of web filtering in the country. However, it tested only a sample of websites and did not include child pornography in the list of content categories tested.

Content controls may be implemented independently by content and hosting providers. Google, for example, has received legal requests from the Philippine government to remove twenty-eight items from its services between June 2010 and June 2014.[168] Of these, twenty were YouTube videos requested for removal on the

[163] A few government agencies (i.e., ICTO, National Youth Commission, etc.) have expressed interest in signing the declaration. However, because they are state agents, a Memorandum of Understanding (MOU) will be necessary should they sign the declaration, subject to the approval of their respective heads of office.
[164] "PH Is Only Country in Southeast Asia with Internet Freedom — Newsbytes.ph," *InterAksyon*, 29 October 2015, http://www.interaksyon.com/infotech/ph-is-only-country-in-southeast-asia-with-internet-freedom-newsbytes-ph.
[165] "Internet Filtering in Asia in 2006–2007," OpenNet Initiative 2007, https://opennet.net/studies/asia2007.
[166] "Asia Overview," OpenNet Initiative 2012, https://opennet.net/research/regions/asia.
[167] Ibid.
[168] "Google Transparency Report for Philippines," https://www.google.com/transparencyreport/removals/government/PH/?hl=en.

grounds that they constituted defamation, whereas the remaining eight were items on the Blogger blogging service that were identified by government authorities as constituting defamation, government criticism, or impersonation. It is not clear how many of these requests were complied with.

In 2014, Google received four removal requests for defamation. Two were YouTube videos, one was an item from Blogger, and one was a search result.[169] Between 2011 and 21 November 2015, the company received six individual requests for the removal of forty-four specified domains from its search results for supposed copyright violations. Finally, from July to December 2015, four removal requests were submitted to Google, three for defamation and one for drug abuse. Google reported a 0% compliance rate during this period.[170] Prominent social media platform Facebook[171] did not receive any government requests to remove content from January 2014 to December 2014 or from 1 January 2015 to 30 June 2015, respectively. These numbers grew to four data requests (and five user/account requests) between July and December 2015.[172]

Many "illegal activities" offline are now presumed to be illegal online as well (e.g., online gambling). The following are some major trends, where the direct tension between Internet "regulation" and Internet "rights" is evident.

Anti-Obscenity/Pornography

With the Philippines being one of only two countries in Asia with a Roman Catholic majority (the other being Timor Leste), the Catholic Church remains a strong influence in domestic social life. It continues to prevail over the local discourse on "obscenity" and "pornography," leading to the proliferation of laws that seek to proscribe "indecent" content. With rising Internet penetration in the country, this discussion has also gradually shifted to cyberspace.

Child pornography, in particular, is a serious problem, given that the Philippines has been identified as a "producer" country. Authorities have sought to crack down on the proliferation of "cybersex dens," many of which are located in poor areas where children as young as two years old are abused and recorded with web cameras.

According to Virtual Global Taskforce, a group of international agencies fighting against child pornography, the Philippines is among the world's top producers of child porn.[173] In November 2009, Congress passed the Anti-Child Pornography Act, which imposed new rules on domestic ISPs, Internet cafe/kiosk owners, and Internet content hosts. The rules require ISPs to notify authorities within seven days of becoming aware that its services are being used to distribute child pornography. ISPs are also mandated to "install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered."[174] The law forbids hosting such content containing child pornography, and requires hosts to remove any such content within 48 hours of notification and turn over to the authorities information regarding the users who attempted to access this content.[175] The Philippine Chamber of Telecommunications

[169] Ibid.
[170] "Requests to Remove Content Due to Copyright," Google Transparency Report, https://www.google.com/transparencyreport/removals/copyright/.
[171] "Philippines Requests for Data," Google Transparency Report, July–December 2015, https://govtrequests.facebook.com/country/Philippines/.
[172] Ibid.
[173] "PHL Among Top Producers of Child Pornography, International Task Force Says," *GMA News Online*, 17 January 2014, http://www.gmanetwork.com/news/story/344345/news/nation/phl-among-top-producers-of-child-pornography-international-task-force-says.
[174] *Republic Act No. 9775*, http://www.gov.ph/2009/11/17/republic-act-no-9775-s-2009/.
[175] Ibid.

Operators (PCTO), an industry group of leading operators, has raised concerns about the logistical complications in monitoring and blocking such content on their services.[176]

In January 2014, the NTC issued Memorandum Circular 01-01-2014, which provides guidelines for the implementation of the anti-child-pornography law. A copy of the circular obtained by GMA News revealed NTC's directive for all ISPs to install available technology that will block access to or filter websites carrying child pornography materials.[177] It made the Inter-Agency Council Against Child Pornography (IACACP) responsible for providing ISPs with lists of websites to block. ISPs are then required to submit to the IACACP a monthly list of pornographic websites that they have blocked.[178] The directive was considered controversial enough that the NTC was forced to clarify that its objective was specifically for ISPs to block child pornography. In July 2015, the NTC issued another directive (Memorandum Circular 03-07-2015), which laid out the minimum technical requirements that ISPs must have to filter or block access to child pornography.[179]

The contested Cybercrime Prevention Act, as recently upheld by the Supreme Court, continues to penalize the crime of "cybersex," which it defines as "the wilful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favour or consideration." Gender and human rights advocates objected vigorously to the vagueness of the definitions as well as the criminalization of any type of sexuality online—an extension of the anti-obscenity discourse—for being both unimplementable as well as legally questionable.[180]

Online Piracy

House Bill No. 6187, "An act to prohibit online piracy and providing penalties for violation thereof" was introduced at the House of Representatives.[181] Although it did not contain any provisions to block online content, it did seek to prohibit online sharing of copyrighted materials. The bill sought to penalize first-time offenders who illegally download content with a minimum two-year jail sentence and fines ranging from PhP50,000 to PhP150,000 (roughly US$1,000–3,000). The penalty increases for second- and/or third-time offenders. Referred to the Committee on Information and Communications Technology on 23 May 2012,[182] the draconian proposed law was criticized by fellow lawmakers and civil society groups.[183] Fortunately, Congress ended its session with the bill remaining stuck at the committee level. On 2 July 2013, the proposed legislation was filed again by the same legislator. As with its predecessor bill, it remained with the committee from the time it was referred there on 24 July 2013 until the sixteenth Congress adjourned sine die in June 2016.[184]

There remains an additional mechanism for web filtering outside of these recent legislative changes. Additional powers granted to the Intellectual Property Office of the Philippines (IPOPHL) in 2013 give the head of the agency the power to issue a seventy-two-hour restraining order against alleged copyright

[176] "Why PH Telcos Oppose Guidelines on Anti-child Porn Law," *ABS–CBN News*, 5 November 2013, http://www.abs-cbnnews.com/business/11/05/13/ph-telcos-oppose-guidelines-anti-child-porn-law.
[177] "NTC Tasks ISPs to Block Child Porn, but Not All Adult Sites," *Yahoo and GMA News Online*, 17 March 2014, https://sg.news.yahoo.com/ntc-tasks-isps-block-child-porn-not-adult-083804400.html.
[178] NTC Memorandum Circular No. 01-01-2014, 30 January 2014, http://www.gov.ph/2014/01/30/ntc-memorandum-circular-no-01-01-2014/.
[179] Rainier Allan Ronda, "NTC Issues Guidelines to Filter Online Child Porn," *The Philippine Star*, 17 July 2015, http://www.philstar.com/headlines/2015/07/17/1477837/ntc-issues-guidelines-filter-online-child-porn.
[180] See Liza Garcia, "Sexuality, Sexual Rights, and the Internet in the Philippines," Global Information Society Watch 2015 (APC and Hivos), https://www.giswatch.org/en/country-report/sexual-rights/philippines.
[181] http://www.congress.gov.ph/legisdocs/basic_15/HB06187.pdf
[182] http://www.congress.gov.ph/legis/search/hist_show.php?congress=15&save=0&journal=1&switch=0&bill_no=HB06187.
[183] Patrick Villavicencio, "Bill Filed to Curb Online Piracy in the Philippines," *Interaksyon*, 19 July 2012, http://www.interaksyon.com/infotech/bill-filed-to-curb-online-piracy-in-the-philippines.
[184] See http://www.congress.gov.ph/legis/search/hist_show.php?congress=16&save=0&journal=1&switch=0&bill_no=HB00915.

violators.[185] These powers were invoked in June 2013 when the domain of popular file-sharing site "Kat.ph" was seized by the IPOPHL following a complaint filed by the Philippine Association of the Record Industry Inc.[186] The seventy-two-hour restraining order was extended to twenty days, and by 13 June the website operators had switched domains.[187]

Cybersecurity and Cybercrime

Challenges to security posed by cybercrime and "cyber terror" pushed many governments around the world to produce legislation as a response to the threat. The Philippines enacted its version of an anti-terror law—Republic Act No. 9372, also known as the Human Security Act of 2007.

Cyber security became a pressing issue since the "I Love You" virus incident in 2000. The virus became a key driver in the passage of a domestic e-commerce law with antihacking provisions.[188] According to the Philippine National Police (PNP), they have received more than 1,200 complaints related to cybercrime in the 2013–2015 period, many of which are incidents of online scams and "online libel."[189]

Concerns regarding cyber warfare fuel the security sector's continuing efforts to beef up national cybersecurity initiatives. For example, international tension with China over disputed islands in the South China/West Philippine Sea has led to various hacking incidents perpetrated by nationals from both countries against each other.[190] To date, the government continues to develop measures to counteract perceived cyber threats by developing and updating cybersecurity frameworks. Intergovernmental bodies, such as the ITU and the Asia Pacific Economic Cooperation (APEC) are also concerned with the issue, providing regional and international avenues for Philippine cybersecurity efforts.[191]

The Council of Europe's cybercrime treaty became the template for the controversial Cybercrime Prevention Act.[192] In February 2014, the Supreme Court came out with its decision on the constitutionality issue, upholding many of the law's contested provisions. The decision received mixed reactions. Law enforcement authorities welcomed the judgment and considered the law as crucial in their operations against online criminals. For the groups that led the protests against the law, the outcome did little to assuage public concerns about the dangers posed by the law's surviving provisions. In the case of online libel, for instance, a broad range of advocates viewed the provision as "a continuing threat against free speech" and "another huge step back for freedom of expression."[193] In September 2014, a woman was formally charged with the offence for

[185] J.M. Tuazon, "Kat.ph Seizure Raises Specter of Cybercrime Law's 'Takedown Clause,'" *InterAksyon*, 17 June 2013, http://www.interaksyon.com/infotech/kat-ph-seizure-raises-specter-of-cybercrime-laws-takedown-clause.
[186] Ben Arnold O. De Vera, "Gov't Takes Down 'Torrent' Website for Illegal Downloads of OPM," *InterAksyon*, 14 June 2013, http://www.interaksyon.com/business/64078/govt-takes-down-torrent-website-for-illegal-downloads-of-opm.
[187] Request for Submission of Comments for the 2014 Special 301 Review, from Director General Ricardo Blancaflor, Philippines Intellectual Property Office, to Ms. Susan F. Wilson, Director of Intellectual Property and Innovation, Office of United States Trade Representative, http://www.ipophil.gov.ph/images/IPEnforcement/CommentofGRPre2014Special301Review.pdf.
[188] RA 8792, the *Philippine Electronic Commerce Act* of 2000.
[189] "Top Five Cybercrimes Complaints in the Philippines, According to PNP," *GMA News Online*, 27 August 2015, http://www.gmanetwork.com/news/story/534597/scitech/technology/top-5-cybercrimes-complaints-in-the-philippines-according-to-pnp.
[190] See, for example, "Filipino Hackers Deface Chinese Websites," *Rappler*, 20 May 2014, http://www.rappler.com/nation/58431-anonymous-ph-hacks-chinese-websites
[191] See, for example, Noelle Francesca De Guzman, "Proposed APEC Cybersecurity Framework Gains Momentum at TEL 52," *Internet Society*, 11 November 2015, https://www.Internetsociety.org/blog/asia-pacific-bureau/2015/11/proposed-apec-cybersecurity-framework-gains-momentum-tel-52.
[192] Various versions of cybercrime legislation were filed in three previous Congresses, but were never passed because of constant scrutiny by human rights advocates and progressive legislators.
[193] Buena Bernal, "SC Rules Online Libel Constitutional," *Rappler*, 18 February 2014, http://www.rappler.com/nation/50881-sc-upholds-cybercrime-law-sections.

allegedly maligning a single mother on Facebook.[194] In 2015, following the issuance of the law's implementing rules, several cases were also filed against a local fashion blogger for supposedly defamatory posts on his Twitter and blog accounts.[195]

Lawmakers were quick to file proposals to amend the cybercrime law's controversial provisions, particularly on online libel. These have coincided with related bills that seek to decriminalize libel, in general.[196] Even the Justice Department, shortly after the Supreme Court came out with its ruling, went on record indicating their intention to submit a recommendation to remove the provision on Internet libel from the cybercrime legislation.[197]

Network Measurement Tests

Internet censorship is now a common occurrence across much of the world, and is especially prevalent in southeast Asia. While the Philippines does not have an extensive history of online censorship, recent legal and regulatory debates about filtering of online content have brought renewed attention to the issue. To identify whether web content is being blocked, as well as to determine the methods used for such blocking, we conducted network measurement tests in the country using the ICLab platform.[198]

These tests consist of running a software tool that attempts to access two predefined lists of websites: the Alexa "top 500" list of the most visited websites worldwide, and a custom list we compiled that consists of 176 URLs relevant specifically to the Philippines, including independent news, human rights, dating, LGBT, political criticism, and file-sharing websites.[199] Our testing list does not contain child exploitation content. We analyzed the results of these tests to determine whether any of the tested content has been filtered. Tests were repeated to distinguish between deliberate filtering and innocuous technical errors.

We conducted tests on the ISP Bayan Telecommunications on 13 and 14 April, and 5 and 12 May 2016. In total, 676 URLs were tested across the two testing lists, with each URL tested on four different dates. Our analysis of the test results did not identify any instances of web filtering. This result is consistent with prior tests of web filtering run in the country.[200]

COMMUNICATIONS SURVEILLANCE

With the rise of Internet connectivity in recent years, the Philippines finds itself increasingly in an environment conducive to communication surveillance. The most recent confirmation of this state of affairs was the 2015 leak of confidential communication between the notorious Italian hacking firm, Hacking Team, and several parties claiming to represent various law enforcement and intelligence units of the Philippine

[194] Francesca N., "Woman from Cebu: First to Be Charged with Online Libel Under Cybercrime Law," *Kicker Daily News*, 20 September 2014, http://kickerdaily.com/woman-from-cebu-first-to-be-charged-with-online-libel-under-cybercrime-law/.
[195] Cathy Cañares-Yamsuan, "Bloggers Subject to the Same Libel Laws as Journalists, Say Liz Uy's Lawyers," *Inquirer*, 13 November 2015, http://lifestyle.inquirer.net/213066/bloggers-subject-to-the-same-libel-laws-as-journalists-say-liz-uys-lawyers; see also Rosette Adel, "'Fashion Pulis' Arrested Over Deniece Cornejo's Libel Charge," *The Philippine Star*, 12 August 2015, http://www.philstar.com/headlines/2015/08/12/1487269/fashion-pulis-arrested-over-deniece-cornejos-libel-charge.
[196] Louis Bacani, "Senators to Decriminalize Libel in Wake of Anti-Cybercrime Law," *The Philippine Star*, 20 February 2014, http://www.philstar.com/headlines/2014/02/20/1292564/senators-seek-decriminalize-libel-wake-anti-cybercrime-law.
[197] Tetch Torres-Tupas, "DOJ Cybercrime Office Sees No Need For Law Vs Internet Libel," *Inquirer*, 19 February 2014, http://technology.inquirer.net/34382/doj-cybercrime-office-sees-no-need-for-law-vs-internet-libel.
[198] Internet Censorship lab (ICLab), https://iclab.org/.
[199] The full list of tested URLs can be found at Citizen Lab's Github repository at https://github.com/citizenlab/test-lists/tree/master/lists.
[200] "Asia," Open Net Initiative, https://opennet.net/research/regions/asia.

government.[201] The year before that, the government was also forced to admit it had acquired surveillance technology as part of its effort to modernize the country's armed forces.[202]

Such revelations, however, are just the latest of many incidents spanning across several decades that effectively confirm clandestine communication interception activities in the country. And while the perpetrators of such acts often remain anonymous, what has been made abundantly clear is that—with two former presidents already figuring prominently in such incidents—no one is too powerful to be immune from having his or her private correspondence spied on and disclosed to the public.

Incidence of Communication Surveillance

Thus far, the most controversial case highlighting communication surveillance in the country concerned former President Gloria Macapagal Arroyo and her role in the electoral fraud purportedly committed during the 2004 presidential elections. Also known as the "Hello Garci"[203] scandal, it involved a recorded phone conversation between the president and one election commissioner wherein instructions for implementing the electoral offence appeared to have been given.[204] The ensuing public outrage prompted an admission and apology from the president, which was broadcast on live television.[205]

The source of the tape—or the entity who carried out the interception—never became clear because multiple copies surfaced with no one claiming actual ownership. The administration had a copy, as did an opposition lawyer who, in turn, pointed to a former senator as his source. The legislator, however, explained that it was merely sent to him by mail.[206] Nonetheless, most of the attention centred on the version allegedly secured from an agent of the Intelligence Service of the Armed Forces of the Philippines (ISAFP). Despite his initial denial,[207] the agent later admitted to taking part in the surveillance operation dubbed "Project Lighthouse,"[208] and tagged the Military Intelligence Group (MIG) 21 of the AFP as the unit that carried out the activity.[209] He also named other individuals involved in the operation and insisted that an employee of a local telecommunications company was also complicit in the illegal activity. The company denied any knowledge of the operation.

Although a legislative inquiry was launched to investigate the incident, it was later terminated for lack of sufficient evidence and remains unresolved to this day. At some point, the president had barred members of the executive department from testifying in congressional hearings without her permission.

---

[201] See Hacking Team, "R: Action Stations As Cyber Attacks on Australia Soar," Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/605081; Hacking Team, "Re: ISS Kuala Lumpur 2012," Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/17209; Hacking Team, "Re: Galileo," Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/17032; Hacking Team, "9th PROTECT International Conference with Specialized Exhibit," Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/351946.

[202] "Palace: Spy Gadgets Are For Anti-terrorism, Not For Prying on Opposition," *Interaksyon*, 11 April 2014, http://www.interaksyon.com/article/84568/palace-spy-gadgets-are-for-anti-terrorism-not-for-prying-on-opposition.

[203] In reference to former Election Commissioner Virgilio Garcillano, who was widely believed to be the person on the other line.

[204] Lawrence de Guzman, "What Went Before: 'Hello Garci Scandal' Investigation," *Inquirer*, 22 July 2011, http://newsinfo.inquirer.net/27379/what-went-before-%E2%80%98hello-garci-scandal%E2%80%99-investigation.

[205] Ibid.

[206] Ibid.

[207] Ibid.

[208] "Doble: 'Hello *Garci'* Wiretap Ops Done Through *Smart* Mole," *GMA* News Online, 22 August 2007, http://www.gmanetwork.com/news/story/57157/news/nation/doble-hello-garci-wiretap-ops-done-through-smart-mole.

[209] "The Tangled Tale of the Tapes," *The PCIJ Blog*, 23 August 2007, http://pcij.org/blog/2007/08/23/the-tangled-tale-of-the-tapes.

Another former president, Corazon Aquino, became the subject of at least two surveillance-related incidents. In 1986, during her visit to the US, a call made to two members of her Cabinet was captured and recorded.[210] An opposition politician leaked the transcript of their conversation days before the ratification of the country's new constitution. The transcript exposed concerns harboured by the administration regarding the impact of the new constitution and its ban on nuclear weapons, especially as it pertains to the fate of the two US military bases in the country.[211] In 2007, surveillance equipment targeting Aquino's private residence was also discovered.[212] Their denials notwithstanding, both the police and the ISAFP were considered the principal suspects in the wiretap.[213] As was the case in "Hello Garci," telco personnel were again alleged to have cooperated. Unlike the 1986 episode, however, no clear reason for the intercept was offered.[214]

Another confirmed wiretapping incident occurred in 2008, when the phone conversation between two witnesses to a graft-laden, albeit botched, government project with China was captured on record.[215] While no one admitted to carrying out the surveillance operation, a copy of the recording wound up in the hands of the chairman of the elections commission, who was then being implicated in the controversial project.[216] The witnesses accused the official of attempting to dissuade them from testifying by threatening to make public their private conversation.[217] As they went ahead with their exposé, the recording was posted online to *YouTube*.

Around the same time, another vocal critic of the administration filed a case against the government. The suit was an attempt to halt a state-sponsored military surveillance operation he believed he was subject to. Guillermo Luz, a prominent business executive, filed petitions for the writs of habeas data and amparo with the Supreme Court. When his petitions were granted, the case was remanded to the appellate court for hearing.[218] The case came to an abrupt end when the armed forces certified that the businessman was not subject to any surveillance or case-building activity.[219]

Other reports involving the anti-wiretapping law turned out to be false alarms. In one case, a legislator was accused of having violated the law after recording an executive session of a Congressional committee.[220] In another, a government executive filed charges against a well-known Filipino journalist for allegedly recording their phone conversation without her consent.[221] Both incidents were eventually resolved, with no case being filed against the legislator. The one filed against the journalist was later dropped, after prior consent of the

---

[210] Keith B. Richburg, "Aquino Aide Accuses Military, US of Tapping Telephones," *The Washington Post*, 27 January 1987, http://www.washingtonpost.com/archive/politics/1987/01/27/aquino-aide-accuses-military-us-of-tapping-telephones/48872f12-8c38-4076-82c8-cdae7db2afec/.

[211] Mark Fineman, "Military Secretly Tapped Aquino's Telephone Calls," *Los Angeles Times*, 24 January 1987, http://articles.latimes.com/1987-01-24/news/mn-9618_1_military-intelligence.

[212] "Ping says Isafp behind Cory Aquino wiretap," *GMA Network*, 04 May 2007, http://www.gmanetwork.com/news/story/40975/news/nation/ping-says-isafp-behind-cory-aquino-wiretap.

[213] Ibid.

[214] "AFP Denies Hand in Cory Wiretap," *GMA News Online*, 3 May 2007, http://www.gmanetwork.com/news/story/40846/news/nation/afp-denies-hand-in-cory-wiretap; see also Jess Diaz, "Lacson Tags ISAFP in Wiretapping of Cory House," *Philippine Star*, 5 May 2007, http://www.philstar.com/headlines/397198/lacson-tags-isafp-wiretapping-cory-house.

[215] "Yet Another Alarming Case of Wiretapping," *The PCIJ Blog*, 23 February 2008, http://pcij.org/blog/2008/02/23/yet-another-alarming-case-of-wiretapping.

[216] Ibid.

[217] Ibid.

[218] "Businessman, Activist Get Habeas Data From SC," *ABS-CBN* News, 12 March 2008, http://www.abs-cbnnews.com/nation/03/12/08/businessman-activist-get-habeas-data-sc.

[219] Mike Frialde, "CA Orders Esperon to Prove Luz Not Under Surveillance," *The Philippine Star*, 14 April 2008, http://www.philstar.com/headlines/55818/ca-orders-esperon-prove-luz-not-under-surveillance.

[220] Angela Casauay, "Tinio Breached Congress Protocol, Trust in Impeach Meeting," *Rappler*, 12 August 2014, http://www.rappler.com/nation/66000-congress-tinio-breach-protocol-recording-executive-session.

[221] "Philippine Reporter Faces Wiretapping Charges," Committee to Protect Journalists, 25 June 2009, https://cpj.org/2009/06/philippine-reporter-faces-wiretapping-charges.php.

complainant was properly established.

Surveillance Technologies

The Philippine government and its intelligence agencies have remained silent regarding the true extent of the state's communication surveillance capabilities. Available literature on the subject has also been relatively scant, if not non-existent. In the past couple of years, however, fragments of information leaked to the public have allowed us a glimpse of some types of technologies the government either has access to, or has at least taken particular interest in.

Remote Control System: Governmental Spyware

Hacking Team's (HT) Remote Control System (RCS) is a powerful surveillance tool designed to monitor a particular device through the direct installation of a malicious program or agent.[222] Once embedded on the device, it is able to collect data practically undetected and untraceable to any encryption technology installed.

While the existence (and use) of the tool in the country cannot yet be substantiated, leaked HT documents have revealed significant interest in the system by parties claiming to represent different agencies of the Philippine government. On 13 March 2011, in response to an inquiry made by an employee of the National Bureau of Investigation's (NBI) Cyber Center regarding a possible solution to cyber attacks, HT outlined the prominent features of RCS.[223] On another occasion, a private individual attempted to set up a meeting between HT and his supposed principal, a city police chief, for the purpose of demonstrating the RCS's capabilities.[224] In 2015, another request for a product demonstration was made by a person claiming to be an officer of the ISAFP.[225] No data are currently available about whether any such interests ended up in an actual sale.

Signal: Social Media Monitoring

Its developers refer to Signal as an online social media monitoring-and-intelligence solution meant for public safety, law enforcement, corporate security, and large-event and emergency management.[226] It processes real-time crowd-sourced information from users' posts in social media platforms, along with other input and user behaviours, to visualize communication information. This, in turn, enables authorities to respond to criminal activity, gather evidence, and even identify potential witnesses and social areas of interest. Reaction time to emergencies is also enhanced, while allowing authorities to communicate more effectively with the public.

Today, the technology is reportedly used by the Royal Malaysian Police and a number of local police units in Australia and the US.[227]

Based on documents disclosed to privacy advocates, a meeting was held between the Philippines government and that of New Zealand early this year to showcase the technology's key features. The tool was described as crucial in harnessing social media for intelligence gathering, threat identification, and real-time investigations. Nonetheless, even as the NZ government has expressed its readiness to support the Philippines's purchase of the technology, no proof is currently available that such a transaction has in fact taken place.

[222] Citizen Lab, "Mapping Hacking Team's 'Untraceable' Spyware," https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.
[223] "R: Action Stations As Cyber Attacks on Australia Soar," Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/.
[224] "Re: ISS Kuala Lumpur 2012," Hacking Team, Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/17209.
[225] "Re: Galileo," Hacking Team, Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/17032.
[226] Signal, http://www.getsignal.info.
[227] Ibid.

Spectrum: Radio Frequency Test Equipment

In early 2014, the Philippine government's purchase of a PhP135M (US$3.4M) Radio Frequency Test Equipment (RFTE)—identified only as "Spectrum" in relevant government records—from German electronic surveillance company Rohde and Schwarz attracted significant public scrutiny. The equipment was described as consisting of "portable analyzers and handheld monitoring receivers for the general purpose of signal investigation and scalar networking,"[228] with the ability to collect massive amounts of information from such varied sources as emails, social media posts, text messages, and cellphones. A subsequent report also characterized the device as capable of monitoring distant radio frequencies "running on certain protocols such as phones, handheld radios, and Wi-Fi devices, and anything that produces radio frequencies,"[229] and as quite resistant to existing countersurveillance technology. Full operational capacity was expected sometime between June and August 2014.

Without any corroborating evidence to substantiate its claims, the exposé alleged that the tool was to be used primarily for spying on critics of the administration, including their families and minor children. It was supposed to give the Aquino government political advantage in the 2016 presidential elections.

While public outcry was kept to a minimum, the conflicting statements made by government officials did court some controversy. Initial denials and vague statements made by those asked to comment on the subject were later supplanted by open admissions, supported by general justifications and assurances.[230] To date, there has been no confirmed use of the equipment in the field, and/or in any law enforcement or military operations.

PISCES: Border Control System

A border-control system that allows the tracking, identification, and detention of suspected terrorists in entry and exit points of a country[231] was also reported to be used in one Philippine airport. The Personal Identification Secure Comparison and Evaluation System (PISCES) was developed by Booz Allen Hamilton, Inc. for the US government's Terrorist Interdiction Program.[232]

Leaked documents show that a Memorandum of Intent was drafted between the US government and the Philippines in 2014 containing the arrangements for the receipt and use of the system by the Philippines. However, despite the leaked documents and the news in 2004 and 2007[233] supporting its existence and use, the Philippine government has yet to confirm this.

---

[228] "P135-M Spy Gadgets Trained on Opponents," *Daily Tribune*, 7 April 2014, http://www.tribune.net.ph/headlines/p135-m-spy-gadgets-trained-on-opponents.

[229] Charlie V. Manalo, "RP Now a 'Big Brother' State—UNA," *Tribune*, 12 April 2014, http://www.tribune.net.ph/headlines/rp-now-a-big-brother-state-una.

[230] Mario J. Mallari, "ISAFP Won't Engage In Politics Through Spyware—Intel Chief," *Daily* Tribune, 8 April 2014, http://www.tribune.net.ph/headlines/by-mario-j-mallari-despite-its-history-of-tapping-telephone-conversations-and-engaging-in-surveillance-operations-on-administration-critics-and-opposition-personalities-which-have-been-proven-under-previous-administrations-the-intelligence-servi; "Noy Dares Critics: Prove Spy Tools' Use vs Political Foes," *Daily Tribune*, 11 April 2014, http://www.tribune.net.ph/headlines/noy-dares-critics-prove-spy-tools-use-vs-political-foes.

[231] "Terrorist Interdiction Program (TIP)" Fact Sheet (2002), Office of Counterterrorism of the US Department of State, http://2001-2009.state.gov/s/ct/rls/fs/2002/12676.htm.

[232] "Federal Investigation Agency," Project Gutenberg Self-Publishing Press, http://www.self.gutenberg.org/articles/federal_investigation_agency.

[233] Sandy Araneta, "BI-NAIA to Create Anti-terror Task Force," *The Philippine Star*, 15 August 2004, http://www.philstar.com/metro/261297/bi-naia-create-anti-terror-task-force; Shaun Waterman, "Americans P*laced on Filipino Watch List*," International Labor Rights Forum, 12 October 2007, http://www.laborrights.org/in-the-news/americans-placed-filipino-watch-list.

Government Surveillance Framework

Attempting to map the Philippine government's intelligence framework is a near-impossible task, given the number of agencies performing surveillance functions and having seemingly overlapping mandates. The maze-like hierarchy is further complicated by rivalries and reported infighting between the institutions themselves, which are made up mainly of military personnel, police officers, and retired members of both uniformed services.

Occupying the apex appears to be the National Security Council (NSC), which is the lead government agency that coordinates the formulation of policies relating to national security[234] and makes recommendations to the president,[235] including the domestic, foreign, military, political, economic, social, and educational policies affecting national security.[236] It has administrative supervision over the National Intelligence Coordinating Agency (NICA),[237] and provides guidance and direction to the operations of the Philippine Center on Transnational Crimes (PCTC).

Engaged in a similar function is the Office of the National Security Adviser (ONSA). The National Security Adviser is a member of the NSC, including its executive committee. In such a capacity, it advises the president on matters pertaining to national security and implements his/her decisions or policies that have a bearing on national security.[238] In 2006, the ONSA was given the principal authority to supervise the build-up and use of reconnaissance and surveillance capabilities of civilian agencies and armed services. For this purpose, it was tasked to carry out "measures to coordinate inter-agency requirements and supervise the acquisition of reconnaissance and surveillance equipment, including but not limited to unmanned aerial vehicles (UAVs)."[239]

The NICA, on the other hand, functions under the Office of the President, and is under the administrative supervision of *both* the NSC[240] and the ONSA.[241] Originally created in 1949,[242] its current mandate is to be "the focal point for the direction, coordination and integration of government activities involving intelligence, and the preparation of intelligence estimates of local and foreign situations for the formulation of national policies by the President."[243] It was reorganized in 2002 before being strengthened the following year when its director general (DG-NICA) was assigned as principal adviser to the president on Intelligence.[244] The agency may detail "liaison officers" to other government offices both inside and outside the country.[245] For this purpose, it coordinates with other government agencies that regularly post representatives overseas.[246] At the same time, through its DG, it is also expected to establish and strengthen liaison work between the agency and its foreign counterpart intelligence and security organizations.[247] In 2006, it was designated as the technical operator of the Maritime Aerial Reconnaissance and Surveillance (MARS) Program.[248] This authorized the agency to "procure UAVs or enter into lease agreements governing such vehicles."[249]

[234] Exec. Ord. No. 292, Book IV, Title VIII, Subtitle I, Chapter 2, § 3 (1987).
[235] Ibid., § 5(3) (1987).
[236] Ibid., § 5(1) (1987).
[237] Exec. Ord. No. 246, § 5 (1987).
[238] Exec. Ord. No. 292, Book IV, Title VIII, Subtitle I, Chapter 2, § 8 (1987).
[239] Exec. Ord. No. 492, § 1, (2006).
[240] Exec. Ord. No. 246, § 5, (1987).
[241] Exec. Ord. No. 69 (2002); see also Admin. Ord. No. 68, § 5 (2003).
[242] See "Brief History," NICA, http://www.nica.gov.ph/about-us.
[243] Exec. Ord. No. 246, § 2 (1987).
[244] Admin. Ord. No. 68, § 1 (2003).
[245] Ibid., § 3 (2003).
[246] Ibid., § 4 (2003).
[247] Ibid.
[248] Exec. Ord. No. 492, § 3 (2006).
[249] Ibid.

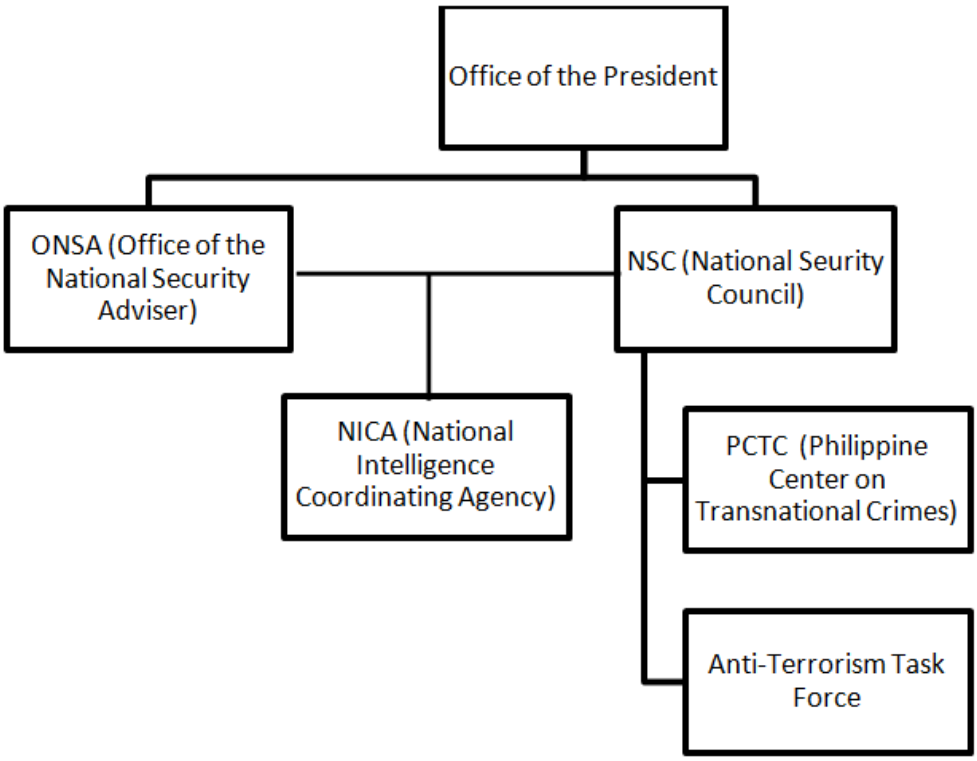

Figure 1 Government Surveillance Organizational Framework

The Armed Forces of the Philippines (AFP) and the Philippine National Police (PNP) are both known to maintain multiple intelligence units whose mandates and full range of technical capabilities have been effectively kept hidden from the public. In the course of this study, for instance, data gathered on the Intelligence Service of the Armed Forces of the Philippines (ISAFP) have been practically nil, apart from it being one of the AFP's Wide Support and Separate Units (AFP-WSSU). The same is true for the Directorate for Intelligence (Directorial Staff) of the PNP. However, the directorate still has its Intelligence Group, which is one of several operational support units.[250] The outfit serves as the institution's intelligence and counterintelligence operating team.[251] According to at least two news reports, this unit (specifically, its counterintelligence component) is also charged with providing physical security to police camps and official documents.[252] It also monitors the illegal activities of police officers.[253] The Anti-Cybercrime Group (ACG) is a recent addition to the PNP after it was directed by the country's cybercrime law to "organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations" of the law.[254] Today, it serves as the primary police unit responsible for the implementation of pertinent laws on cybercrime and anti-cybercrime campaigns of the PNP and the national government, including the surveillance component

[250] Rep. Act No. 6975, § 35.
[251] Rep. Act No. 6975, § 35(b)(2).
[252] See Dennis Carcamo, "*Purisima to Abolish PNP's Counter-intelligence* Unit," *The Philippine Star*, 18 January 2013, http://www.philstar.com/headlines/2013/01/18/898440/purisima-abolish-pnps-counter-intelligence-unit; Jamie Marie Elona, "*Purisima* Eyes Disbanding *PNP* Intelligence Unit," Inquirer, 18 January 2013, http://newsinfo.inquirer.net/342853/purisima-eyes-disbanding-pnp-intelligence-unit.
[253] Ibid.
[254] Rep. Act No. 10175, § 9.

of the cybercrime statute.[255]

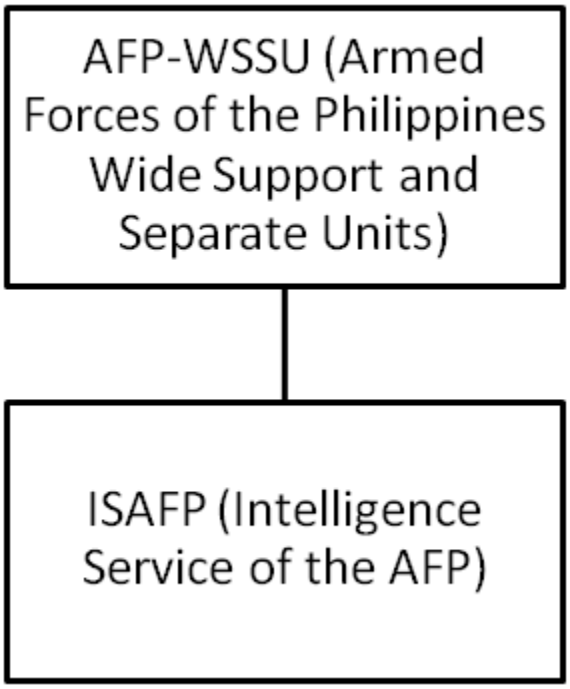

Figure 2 AFP-WSSU and ISAFP Relationship

Outside of the PNP, which is an attached agency of the Department of the Interior and Local Government, a handful of offices belonging to the justice department also perform intelligence functions. The DOJ's newly minted Office of Cybercrime (OOC), for example, has been tasked to serve as the central authority in all cybercrime matters related to international mutual assistance and extradition.[256] It is also responsible for coordinating the efforts of the National Bureau of Investigation (NBI) and the PNP in enforcing the provisions of this law.[257] The NBI's Cyber Crime Division (CCD), which falls under the Office of the Deputy Director for Investigation Services,[258] was also established in compliance with the cybercrime law and given the same powers[259] as the ACG of the PNP. Both the PNP-ACG and NBI-CCD are required by the act to submit pre-operation, post-operation, and investigation results to the DOJ-OOC for review and monitoring. [260] At the same time, the NBI's Office of the Deputy Director for Intelligence Services remains in operation. The Intelligence Services units falling under this office include: Counter Intelligence Division (CID); Criminal Investigation Division (CRID); and the Technical Intelligence Division (TID).[261]

[255] See PNP Directorate for Operations, "*PNP Activates Anti-Cybercrime Group*", Philippine National Police, http://acg.pnp.gov.ph/main/index.php/press-releases/39-pnp-activates-anti-cybercrime-group (last visited 25 October 2015); Dennis Carcamo, "PNP Forms Anti-Cybercrime Group Despite TRO," *The Philippine Star*, 20 March 2013, http://www.philstar.com/headlines/2013/03/20/922017/pnp-forms-anti-cybercrime-group-despite-tro.
[256] "Vision, Mission, Pledge, Mandate and Functions," Republic of Philippines Department of Justice, https://www.doj.gov.ph/vision-mission-and-mandate.html.
[257] "Powers and Functions," Office of Cybercrime, Department of Justice, https://www.doj.gov.ph/office-of-cybercrime.html.
[258] "NBI Divisions," National Bureau of Investigation, http://www.nbi.gov.ph/divisions.html.
[259] Rep. Act No. 10175, § 10.
[260] Rep. Act No. 10175, § 11.
[261] National Bureau of Investigation, see note 56.

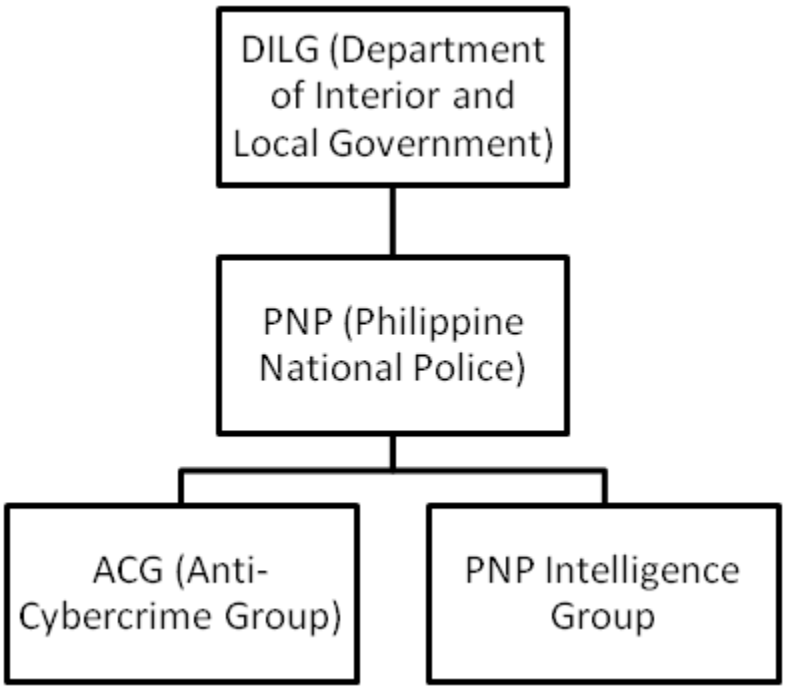

Figure 3 DILG and the PNP

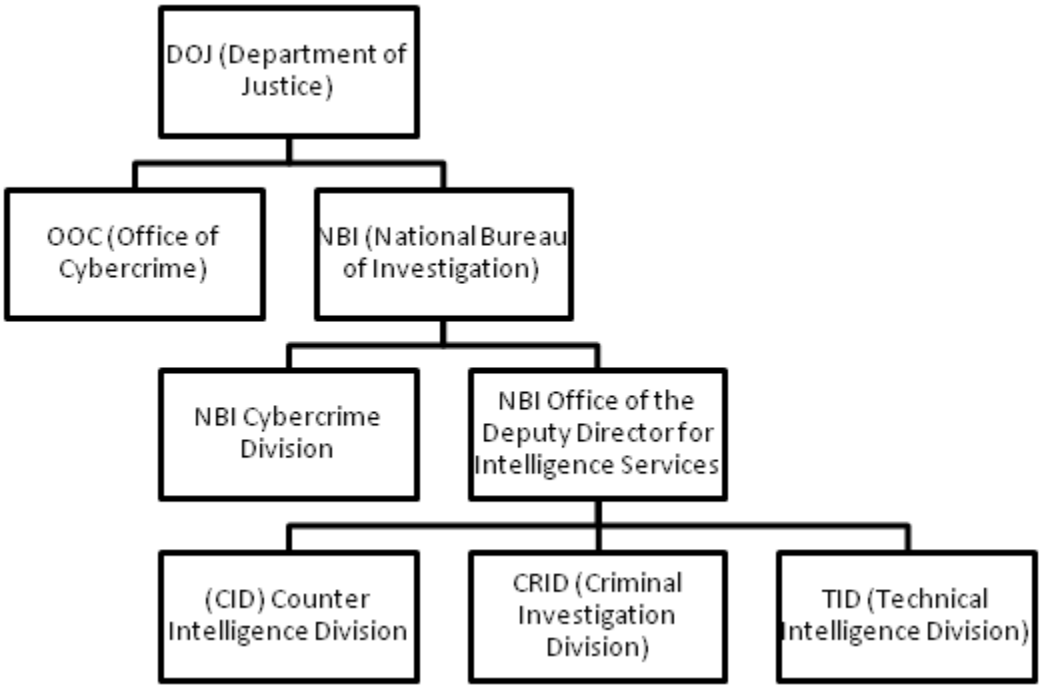

Figure 4 DOJ Divisions

In 2014, there were reports regarding a plan by the government to create a new intelligence agency similar to that of the US Defense Intelligence Agency,[262] which would supposedly incorporate the ISAFP as an integral

[262] "P135-M Spy Gadgets Trained on Opponents," *Daily Tribune*, 7 April 2014, http://www.tribune.net.ph/headlines/p135-m-spy-gadgets-trained-on-opponents.

part of the Philippines's defence department. The new agency would engage in the "gathering and analysis of security-related foreign, domestic, political and economic, industrial, geographic, military and civilian intelligence data."[263] The plan was allegedly scuttled because of fundamental differences between the merging institutions.

PRIVACY RIGHTS

While the Philippine Constitution protects the privacy of communications and the security of persons, homes, and papers,[264] the country has never had a data protection law that sets forth the rights of data subjects. This gap has become increasingly problematic in recent years with the advancement of technology, and with vast amounts of personal data now online. The policy gap has become more prominent and now poses a major challenge to privacy rights everywhere.

Corporate Control of Personal Data

Online transactions and social media use mean that there are increasing amounts of sensitive personal information in the hands of private companies. Social media companies, in particular, are sitting on a treasure trove of personal data handed over by people in exchange for free services. In so doing, the companies have successfully taken away data ownership and control from their original owners. Online and offline retailers are also keeping vast amounts of consumer transaction and personally identifiable data. Even service institutions such as health providers possess sensitive personal information with very little oversight on how they use or repurpose user data. Many private companies retain personal data for long periods of time without oversight from any public authority; the usual reason given for this is for "billing purposes" and for "marketing studies."[265]

In the course of its earlier work with Citizen Lab in the OpenNet Asia Network, FMA explored how private corporations—particularly telecommunications companies—have come to dominate the domestic ISP space. Telcos have now become particularly powerful gatekeepers because they are almost the single point of contact for many citizens communicating through their phones. All text/SMS, voice, and, increasingly, Internet data (over smartphones) now pass through telcos, which has given rise to problematic incidents where personal information was compromised.

Some Internet companies have been involved in traffic shaping and content throttling, particularly in cases where peer-to-peer networking is involved over their networks, and have "invisible" data caps in place on what are marketed as "unlimited" data packages to consumers.[266] Aside from quality-of-service concerns that are directly related to the growing backlash against slow and expensive Internet service in the country, these cases imply corporate practices of "deep packet inspection," which crosses beyond the privacy issue into more complex "network neutrality" concerns that are only recently being explored.

In the Philippines, rights-informed (and comprehensible) end-user policies are absent, and privacy policies remain inadequate at ensuring the protection of users' privacy rights. Disclosure regimes do not exist, and transparency reports are not mandatory in the absence of clear privacy regulations and rules.

[263] Ibid.
[264] 1987 Philippine Constitution. Article III, Sections 2 and 3.
[265] This is drawn from conversations with telecommunication company insiders who will have to remain anonymous for now.
[266] See, for example, Abe Olandres, "Bandwidth Caps Out; Is Throttling next?" *YugaTech*, 18 January 2011, http://www.yugatech.com/telecoms/bandwidth-caps-out-is-throttling-next/.

Slow Implementation of Data Privacy Act

For many CSOs who campaigned for the passage of the privacy rights law, a National Privacy Commission was seen as critical to ensure accountability and transparency in the processing of private personal information by both state and nonstate actors. This was the hope when the *Data Privacy Act* was passed, however, after more than three years since the law passed, the Implementing Rules and Regulations (IRR)—the operational framework of any law that is drafted soon after its passage—have not been implemented.[267] This is because of delays in the creation of the NPC, which is the agency officially tasked with drafting such rules.[268]

ICTs have been vital in providing communications access for a large segment of the population. However, this private-sector-led ecosystem, coupled with a weak state, has brought forth new regulatory challenges. The dominant influence wielded by large corporations, coupled with a weak regulatory framework both in leadership and policy development, have exposed serious gaps in consumer protection capabilities by the state and its capacity to implement sound ICT policies. The emerging challenges to human rights in a digital world powered by fast-changing technologies have caught the Philippine state unprepared.

AREAS FOR FURTHER STUDY

To date, a comprehensive and thorough understanding of the Philippine surveillance landscape remains elusive. In the absence of any information on the policies and guidelines that state agencies subject themselves to (outside of the statutes passed by Congress) there is very little opportunity for critics, privacy advocates, and the public at large to engage in a meaningful discussion of the subject, especially with regard to its impact on equally relevant concerns such as human rights.

Nevertheless, a number of useful facts may be gleaned from what little data are currently available. First, there are many state agencies that operate with intelligence-gathering functions, which appear to have overlapping and/or redundant mandates. Worse, apart from the regular courts, there is practically no direct oversight mechanism that could establish a clear boundary between lawful and unsanctioned surveillance and ensure that state agents are bound by legal restraints. Second, the existing legal regime that is supposed to rein in potential abuse or misuse of surveillance is also very weak. Not only does this weakness allow for serious regulatory gaps, but it also deprives victims of any reasonable access to justice. Third, new bills that are being proposed in relation to communications surveillance should be tracked and studied.

Consequently, there remains an urgent need to surface more information on this subject that could potentially lead to a transparent and responsible surveillance framework in the country. Only by exposing the fundamental components of such a framework can its current state be accurately assessed. Such evaluation is critical in determining the need for policy and procedural changes, with a view to making the current system more effective and efficient, and in keeping with a strong rights-based system. Political will from those in government and vigilance among the citizens are necessary to bring such aspiration to its full realization.

ENGAGING THE FUTURE OF INTERNET GOVERNANCE: 2017 AND BEYOND

What follows are the key areas that are likely to require particular attention in the field of Internet governance, paired with recommendations for action.

[267] With the support of Privacy International and cooperation from DOST-ICTO, FMA embarked on a series of consultations and roundtables to produce draft IRRs in 2013 up to early 2014. The effort stalled when no one could "receive" the recommendation and draft IRRs produced.
[268] The NPC is composed of a chairperson (with the rank of Cabinet Secretary), and two deputy commissioners with the rank of undersecretary, appointed to a fixed three-year term.

Mainstreaming a Progressive ICT Agenda in Future Elections

Support and build up champions of a progressive ICT agenda among incumbent and future government officials.

2016 was important year for the Philippines as a result of the national elections in May. A number of candidates who ran for top posts in the Philippine government—namely, president and vice president, senators and congressmen, as well local chief executives— expressed their intention to engage in ICT issues. Candidates looking to curry favour with voters claimed to support ICT development and promised to espouse related programs such as addressing the persisting problem of slow and expensive Internet connectivity. Some expressed their support for the Magna Carta for Philippine Internet Freedom, such as Senator Miriam Defensor-Santiago.[269] Still, it was evident during the 2016 election campaign period that very few politicians had the capacity to come up with progressive agendas with regard to cyber security, sexual expression online, and/or favours consolidating rather than breaking telecommunication monopolies in the country. In future elections, it will be crucial for the ICT policy community to support those who have shown and those who will display an understanding of the importance of sound Internet policies and multistakeholder governance.

Embedding Sound Internet Governance in the new ICT Strategic Plan

Build a new ICT master plan that incorporates a clear Internet governance framework that is developed in close consultation with various stakeholders, particularly civil society.

The previous ICT master plan is coming to an end and the ICTO has released an initial assessment and recommendations to guide the post-2016 successor plan, which is dubbed the "National ICT Development Plan 2017–2022."[270]

CSOs should engage the new planning process with renewed vigour, armed with the lessons of the past four years. In developing strategic outcomes, the new plan must have a clear Internet governance framework informed by local experiences and international best practices. It must also engage all stakeholders in crafting and implementing a sound institutional strategy that fills in the gaps of the past and responds to the challenges of the present. In all of this, it is imperative to imbue the successor plan with basic human rights protection in accordance with internationally accepted norms and standards, even as it engages with all future technological possibilities.

Institutional Reform and Development for Sound Internet Governance

Develop the capacity of key ICT institutions such as the Department of Information and Communications Technology (DICT), the National Telecommunications Commission (NTC), the National Cybersecurity Inter-agency Committee (NCIC), and the Cybercrime Investigation and Coordinating Center (CICC).

ICT policy development and regulatory and governance structures are crucial in ensuring sound Internet Governance. It will be important to pay attention to:

- creating capacity for the newly established Department of Information and Communications Technology (DICT), which is poised to replace and absorb the ICTO. This includes ensuring the agency's financial viability and recruitment of competent personnel;[271]

[269] Norman Bordadora, "Santiago proposes Magna Carta for Internet Freedom," *Inquirer Technology*, https://technology.inquirer.net/20769/santiago-proposes-magna-carta-for-internet.
[270] ICTO convened an initial multistakeholder meeting in October 2015 to present its PDS assessment. It also presented an overview of new ICT Plan's framework was presented to the public on 15 December 2015.

- reforming and restructuring the NTC to insulate it from market capture, as well as enabling it to better respond to current and emerging regulatory challenges;
- building the capacity of the new National Privacy Commission;
- engendering more interagency collaborations, especially in the DICT's case and its relationship with the Commission on Human Rights, Philippine Commission on Women, Commission on Elections, and other sectoral line agencies (Department of Environment and Natural Resources, National Disaster Relief and Rehabilitation Commission, and agencies dealing with PWDs, indigenous people, and other excluded communities);
- engaging the new National Cybersecurity Inter-agency Committee (NCIC) under the Office of the President[272] as well as the Cybercrime Investigation and Coordinating Center (CICC);[273] and
- strategizing for a post-2016 sustainable multistakeholder platform for Internet Governance (i.e., a NICTAC 2.0).

Engaging the Post-2015 ASEAN ICT Master Plan

Develop a post-2015 ASEAN ICT master plan in a more consultative and inclusive manner than previously done, both at the national and regional levels.

The Philippines is part of the Association of Southeast Asian Nations (ASEAN), which established an economic community in 2015. The group had previously developed an ASEAN ICT Master plan or AIM[274] for the period 2010–2015, which identified four key outcomes: (1) ICT as an engine of growth for ASEAN countries; (2) recognition of the ASEAN as a global ICT hub; (3) enhanced quality of life for the ASEAN population; and (4) provision of contributions towards ASEAN integration.

Governments have since crafted and published the ASEAN ICT Master Plan 2020.[275] AIM 2015 was criticized by Internet rights advocates for having been developed and implemented without civil society participation. During the 2015 ASEAN People's Forum in Kuala Lumpur, they demanded that the development of future plans involve civil society in all stages and must be a truly regional process.[276]

On the domestic front, ICTO held a last-minute consultation on 9 September 2015 among local stakeholders regarding their proposed draft. Unfortunately, the week allotted for parties to prepare an official position on the draft proved to be insufficient. In the future, NGOs should be more pro-active about the development and implementation of AIM and gather like-minded organizations across the region to present a unified front in pushing the AIM towards more progressive agendas.

Mainstreaming the PH Declaration on Internet Rights and Principles

Continue developing and popularizing the Philippine Declaration of Internet Rights and Principles, engaging civil society, the technical community, and the private sector in the process.

---

[271] As of the time of publication, the law creating the DICT (RA 10844, *Department of Information And Communications Technology Act of 2015*, http://www.gov.ph/2016/05/23/republic-act-no-10844/) has been passed. Many in the ICT sector lauded this as signalling the strategic importance of ICT in national development. Further, the DICT is a full Cabinet-level department as opposed to just an attached agency of the DOST.
[272] For the creation of the CCIC, see Executive Order No. 189, s. 2015, "Creating the National Cybersecurity Inter-Agency Committee," http://www.gov.ph/2015/09/17/executive-order-no-189-s-2015/. Representatives from nongovernment organizations, the academy, and the private sector have seats in the CCIC. It may invite concerned public and private agencies or entities to participate in cyber security policy discussion.
[273] Mandated by *Republic Act 10175*.
[274] "ASEAN ICT Masterplan 2015 Completion Report," http://www.asean.org/storage/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf.
[275]"The ASEAN ICT Masterplan 2020," http://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf.
[276] "Workshop on Internet, Human Rights and Governance in ASEAN, 21 April 2015, Key Recommendations," Latest News: Updates from the ASEAN Peoples' Forum, http://aseanpeople.org/workshop-on-Internet-human-rights-and-governance-in-asean/.

All the initiatives outlined thus far demonstrate the need for CSO engagement based on a clear vision that advances the desired set of rights and principles. The *Philippine Declaration* is the most advanced document that may be used as a basis for many of the present and future agendas of CSOs.

Currently, stakeholders who shepherded the declaration look forward to mobilizing more CSOs, the technical community, and even the private sector to support and propagate it. This broad participatory process is essential in addressing ICT issues effectively. Civil society must take the lead in getting government and the private sector to listen to grassroots perspectives when dealing with important issues as they chart the future of Philippine ICT. Adding to the original twenty-three signatories to the declaration is essential, as does getting key state agencies and private sector organizations on board. The initial openness of ICTO to the declaration should be leveraged to embed the declaration's key elements in the new ICT master plan.[277]

That said, the PH Declaration, though very significant, remains an open document that needs to be developed further. Aside from expanding the existing set of signatories and popularizing the document for different constituencies (and possibly in different local languages), CSOs will have to extend the research and development work on the declaration's main items and operationalize them in the concrete conditions of the Philippine ICT ecosystem.

It is important to ensure that the discourse on Internet governance is not monopolized by government or actors that just happen to have the most resources. The Internet is for all, and therefore must be governed in a manner that reflects this. Critical engagement is the challenge, and all stakeholders must strive to make their voices heard. Winthrop Yu of ISOC PH is particularly optimistic: "We just have to continue engaging the process and help in increasing the awareness of decision-makers of the positive impacts in the economy of an inclusive multi-stakeholder Internet governance model."[278] To see such optimism realized, civil society will have its work cut out for itself in the next couple of years. Despite the high level of difficulty, the stakes are significant enough that there is no option other than to try.

ACKNOWLEDGEMENTS

This research was made possible by the generous support of Hivos Southeast Asia.

Research and writing was completed by Al Alegre, Nica Dumlao, Jamael Jacob, Jessamine Pacis, and Randy Tuano of the Foundation for Media Alternatives (FMA), and Irene Poetranto, Adam Senft, and Amitpal Singh of the Citizen Lab at the Munk School of Global Affairs, University of Toronto.

Thanks also to Masashi Crete-Nishihata, Ron Deibert, and Jacqueline Larson.

[277] "Launch of the Philippine Declaration on Internet Rights and Principles," http://www.dict.gov.ph/launch-of-the-philippine-declaration-on-internet-rights-and-principles/.
[278] Interview with Winthrop Yu, October 2015