TIKTIK:

An Overview of the Philippine Surveillance Landscape

Surveillance Technologies

Foundation for Media Alternatives

September 2015

About the Organization

The Foundation for Media Alternatives (FMA) is a nonprofit service institution whose mission is to assist citizens and communities—especially civil society organizations (CSOs) and other development stakeholders—in their strategic use of information and communications media towards democratization and popular empowerment.

Since its formation in 1987, the organization has sought to enhance the popularization and social marketing of development-oriented issues and campaigns through media-related interventions, social communication projects, and cultural work. In 1996, FMA streamlined its programs and services in both traditional and new media, directing its focus on information and communications technologies (ICTs). The current thrust of the organization is to enable communities assert their communication rights, while defending their rights to information and access to knowledge, towards progressive social transformation.

About the Report

This Report is a key component of a Project FMA is currently undertaking with Privacy International (PI), an non-governmental organization based in the United Kingdom advocating for privacy rights around the world, and several other organizations operating in thirteen (13) countries, particularly in South and Southeast Asia, East and North Africa, and Latin America. The Project aims to build the capacity of civil society and other change agents in detecting and responding to surveillance activities, by providing knowledge, tools, and resources that allow them to investigate and respond to surveillance technologies operated by both State and private actors. It also seeks to build momentum for policy change, with a view to institutionalizing strong human rights protections in the national surveillance laws of the countries involved.

Sed quis custodiet ipsos custodies?

(But who will guard the guardians themselves?)

— **Juvenal** (c. 60-130 AD)

Contents

Introduction

As privacy scholars are wont to point out, surveillance and spies have been around since the dawn of civilization approximately 5,000 years ago. With the rise and fall of kingdoms and empires, and the rivalries that defined their relations, it was necessary for rulers to not only gather intelligence on the strength and morale of their enemies, but also to assess the loyalty and sentiment of their own people.

Today, little has changed in this regard, with countries continuing to earmark manpower and resources for surveillance towards the ultimate aim of protecting their sovereignty against all threats, both foreign and domestic. As author, Keith Leidler, points out: "Any administration will keep records, and will almost invariably arrogate to itself the right to engage in covert surveillance… should this be deemed necessary for the security of the state".[1] The more comprehensive the scope of the surveillance infrastructure, the more secure a country is perceived to be. At least, this is the narrative State agents would have people believe.

In the case of the Philippines, the recent escalation of Chinese military-led activities in the West Philippine Sea have highlighted the need for a constant and effective monitoring of national borders, particularly those shared with neighboring States. In the local front, the 46-year old communist insurgency, a persistent Muslim separatist movement in the South, and local manifestations of the global war on terrorism, have placed the country's armed forces and law enforcement machinery in a perpetual state of alert. So too has the increasing crime rate, especially with the recent proliferation of Internet- and other ICT-related offenses. On their heels are various surveillance-enabling mechanisms like data retention, biometrics, a national ID system, and mandatory SIM card registration that are now either in place or are being aggressively pushed in Congress to enhance the government's burgeoning surveillance network.

This scenario may now be observed in a host of other countries around the world. It's a phenomenon that is far from being an isolated case of happenstance, for a huge boon for today's governments is the fact that technical barriers to a true surveillance society no longer exist. The emergence of computers, the Internet, electronic intelligence and communications has swept aside the limitations that previously restricted

[1] Keith Laidler, SURVEILLANCE UNLIMITED: HOW WE'VE BECOME THE MOST WATCHED PEOPLE ON EARTH 10 (2008).

visions of an omniscient and omnipresent monitoring system. With the proper tools, it is now possible to follow people wherever they go, listen to their calls, read their correspondences, and eventually form individual profiles, based on their unique personal circumstances. All the while they remain unaware of the fact that they are actually being watched. Meanwhile, the legal mechanisms necessary to curtail abuse of these intrusive capabilities lag far behind the development and introduction of newer, more powerful spywares.

Inevitably, this state of affairs set forth widespread debate between proponents and critics of surveillance. Benefits and downsides have been invoked in equal measure, with neither side willing to concede its position. The role of surveillance in the fight against terrorism and organized crime, as well as in increasing productivity and efficiency in work environments is no longer in doubt. Neither is its potential as an effective tool for discrimination and repression. Unfortunately, in the prevailing narrative, it is the benefits that are often magnified and celebrated, while the inherent risks are routinely glossed over or ignored. This is the danger that requires utmost attention above all else, for if the status quo is maintained, the full extent of surveillance's intrusive nature will never be considered in its frightening entirety, and a truly informed discussion of the subject will never take place.

This Report (and the Project it is part of) seeks to address this problem head on. In taking up specific surveillance systems and devices associated recently with the Philippine government, it recognizes surveillance technology as a Janus entity with both positive and negative uses and consequences. The Project, in particular, seeks to provide the public sufficient data on the phenomenon, its crucial elements, and the issues it gives rise to, allowing for an informed decision on which facet of surveillance they prefer looking their way.

How much surveillance is acceptable in a truly democratic society? When does it exceed its purpose, such that the proposed cure ends up being worse than the disease it was meant to address? Is the public willing to accept the gradual erosion of their fundamental liberties, in exchange for a (perceived) more robust level of security? These are but some of the important questions that need space and time for discussion and this Report offers itself humbly as an opportunity and a worthy start.

Personal Identification Secure Comparison and Evaluation System (PISCES)

PISCES is the acronym for Personal Identification Secure Comparison and Evaluation System, a customizable software application that provides border control officials with information that allows them to identify and detain or track individuals of interest.[2] The system can be used to quickly retrieve information on persons who may be trying to hastily leave a country after committing a crime, or a terrorist incident.[3]

The software was introduced in 1997 through the U.S. government's Terrorist Interdiction Program (TIP),[4] "a highly effective, low-cost proven tool in the global fight against terrorism…. (which) …provides participant countries with the ability to collect, compare and analyze traveler data to assist the country in securing its borders and, if necessary, detain individuals of interest".[5]

Booz Allen Hamilton

The software developer is Booz Allen Hamilton, Inc. (BAH), a Fortune 500 company that describes itself as "a leading provider of management consulting, technology, and engineering services to the US government in defense, intelligence, and civil markets".[6] As such, its principal clients consist of the military, the Department of Homeland Security, the Department of Health and Human Services, the Department of the Treasury, intelligence agencies, as well as civil agencies of the U.S. government. It also claims to extend its services to major corporations, and even not-for-profit organizations.

At the moment, the company is most famous for being the former employer of whistleblower, Edward Snowden. On top of the privacy rights violations and major security lapses made public by the latter's

[2] OFFICE OF COUNTERTERRORISM. FACT SHEET (2002), http://2001-2009.state.gov/s/ct/rls/fs/2002/12676.htm.
[3] id.
[4] *Federal Investigation Agency*, PROJECT GUTENBERG SELF-PUBLISHING PRESS, http://www.self.gutenberg.org/articles/federal_investigation_agency (last visited Sep. 21, 2015).
[5] OFFICE OF COUNTERTERRORISM. supra note 2.
[6] BOOZ ALLEN HAMILTON, BOOZ ALLEN HAMILTON FACT SHEET (2015), http://www.boozallen.com/content/dam/boozallen/media/file/Booz_Allen_Fact_Sheet.pdf.

PISCES 9
Source: http://perkinswill.com/sites/default/files/styles/pw_hero_image/public/project-imagery/BoozAllen_02_PP110812_main_1.jpg?itok=NIOY2CeX

revelations, the over-privatization of many governmental functions, particularly in sensitive policy areas, was also exposed to public scrutiny.[7] This peculiar gaffe in governance has transformed companies like BAH into cash cows, earning billions of dollars from performing government functions for or on behalf of the U.S. government.

Deployment

In 2002, the U.S. provided seventeen (17) countries with the PISCES software. They included Pakistan, Afghanistan and Yemen.[8] By 2005, that number had risen to 21.[9] Azerbaijan initially made use of the system before choosing to discontinue it and replacing it with the Canadian Bank Note Company ID card.[10] Pakistan also discontinued the use of the system in 2011, and replaced it with a locally-developed program.[11]

Despite its initial promise, PISCES has been consistently hounded by technical issues. For instance, the slowdown of the processing of travellers has been a major drawback for many of its users.[12] Its inability to allow integration with the issuance of visas and working permits is another. In fact, one of the key features of its replacement in Pakistan was accessibility for the country's visa-issuing authorities.[13] Senegal was also forced to discontinue its use in 2006 after experiencing a slew of technical difficulties.[14] Immigration officials were often plagued with software and hardware problems that required frequent maintenance services. Without skilled and knowledgeable people to maintain the system, its continued use simply became too costly to sustain.

In addition, its use by the participating countries also took fire from local critics. In the Maldives, direct access by the U.S. to travellers' information through PISCES was the subject of much public outrage when the Defense Minister failed to disclose to the public the full nature of his

[7] Norm Ornstein, *Edward Snowden and Booz Allen: How Privatizing Leads to Crony Corruption*, THE ATLANTIC (Jun. 20, 2013), http://www.theatlantic.com/politics/archive/2013/06/edward-snowden-and-booz-allen-how-privatizing-leads-to-crony-corruption/277052/.
[8] Saba Intiaz, Pakistan to replace 'insecure' US border watch software, THE EXPRESS TRIBUNE (Jun. 8, 2011), http://tribune.com.pk/story/184568/pakistan-to-replace-insecure-us-border-watch-software/.
[9] http://wwwa.house.gov/international_relations/109/pop031005.htm
[10] PARLIAMENT OF CANADA. 37th Parliament, 2nd Session, Standing Committee on Citizenship and Immigration (Apr. 1, 2003), http://www.parl.gc.ca/InfocomDoc/37/2/CIMM/Meetings/Evidence/CIMMEV51-E.HTM.
[11] Intiaz. *supra* note 8.
[12] Azra Naseem, *Meet PISCES: the US Broader Control System*, DHIVEHI SITEE (May 13, 2013), http://www.dhivehisitee.com/executive/us-generosity/.
[13] *Pakistan phases out U.S.-made border monitoring software*, HOMELAND SECURITY NEWSWIRE (Jun. 9, 2011), http://www.homelandsecuritynewswire.com/pakistan-phases-out-us-made-border-monitoring-software.
[14] Naseem, *supra* note 12

government's agreement with the U.S. He had stated that the U.S. could not access data that the Maldivian Government did not want to share. However, the Memorandum of Intent sealing the deal between the two countries belied his claim.[15] Meanwhile, in Pakistan, another reason given by the government for its decision to discard the system was the growing concern over the integrity of local data being processed by a foreign-made and –maintained application.[16] Just recently, Malta's use of PISCES was questioned by Germany on the ground that it poses a security risk to other EU Member States.[17] This sentiment is borne out of the now very public fact that BAH, PISCES's developer, works closely with the U.S. National Security Agency (NSA). Malta is the only member of the European Union to use the border control software.

PISCES and the Philippines

As present, the Philippine government has yet to give an official confirmation regarding its use—past or current—of the PISCES system.

It is worth noting, however, that in 2004, a local daily came out with a report quoting a Bureau of Immigration officer stationed at the Ninoy Aquino International Airport (NAIA) as he remarked about an impending upgrade of the PISCES program they were then using in that facility [18]

Another article in 2007 appeared to confirm such fact after citing the U.S. State Department's admission regarding the deployment of PISCES in two NAIA terminals back in 2004.[19] The article itself concerned the inclusion of 504 Americans in a Filipino watch list—with 69 identified as possessing links to Al-Qaida and/or the Taliban. It was widely condemned by human rights groups in the States as a form of harassment, after claiming that those included in the list were in fact labor and religious advocates with no connection to terrorism. While denying that the PISCES system was used in including the 69 Americans on the watch list, a State Department official did imply that the Philippine government had already stopped using the software, after deciding to "rely on other techniques for watch-listing".[20]

[15] id.
[16] Intiaz. *supra* note 8.
[17] Cornelia Ernst, *Subject: Award of Contracts for IT policing systems to external suppliers*, EUROPEAN PARLIAMENT (Dec. 22, 2014), http://tinyurl.com/np29e7p.
[18] Sandy Araneta, *BI-NAIA to create anti-terror task force*, THE PHILIPPINE STAR (Aug. 15, 2004), http://www.philstar.com/metro/261297/bi-naia-create-anti-terror-task-force.
[19] Shaun Waterman, *Americans placed on Filipino Watch List*, INTERNATIONAL LABOR RIGHTS FORUM (Oct. 12, 2007), http://www.laborrights.org/in-the-news/americans-placed-filipino-watch-list.
[20] id.

Since then, there have been indications that the software is on its way back to Philippine shores. Leaked documents suggest that some time last year, a Memorandum of Intent was drafted between the Philippines and the U.S. government outlining the operational arrangements for the receipt and use by the former of the PISCES software. According to the documents, the U.S., apart from providing the hardware and software necessary to run the system, would also train Filipino personnel for its operation and maintenance. NAIA was identified as the first point/area of installation, to be followed by other locations as designated by Philippine authorities, in coordination with their U.S. counterparts.

The documents also revealed that the concerned Philippine government agencies are generally in favor of the system and its use, even with some expressing concerns, including those issues surfaced by other country experiences, as cited above.

Signal

Societies across the globe have embraced social media at such a rapid pace that it has now become a core part of daily life. Social networks, it turns out, are effective enablers of people's insatiable desire for self-expression and concordant need for communication.

The amount of data produced by these platforms, including the rate this is done, is phenomenal. It did not take long for people to realize that a technology capable of capturing, collating, and processing all this information could be extremely useful in many ways. In recent years, one application has presented itself as capable of filling such need: Signal.

According to its proponents, Signal is an online social media monitoring and intelligence solution meant for public safety, law enforcement, corporate security, large event and emergency management. It filters, searches, maps and integrates real-time crowd-sourced information from users' posts in social media platforms (i.e., Facebook, Twitter, Instagram and YouTube) with other input and user behaviors in order to visualize communication information, through the construction of a composite picture of an ongoing event or incident, or even the day-to-day operations of particular organization.

Initially developed by the New Zealand Police as part of its security measures during the Rugby World Cup hosted by the country in 2011, the application later underwent significant enhancements, owing to the Police's subsequent partnership with Intergen and Microsoft. Among others, all information gathered by the application are now funneled into a single platform known as Real-Time Intelligence for Operational Deployment (RIOD). This platform is based on Microsoft SharePoint[21] and allows for improved collaboration, process optimization and information discovery. Meanwhile, the Microsoft Azure cloud platform is used to secure real-time intelligence and provide situational awareness on specific incidents.

[21] Microsoft, *New Zealand Police* (Jul. 11, 2014), https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=2249.

How it Works

The software is available for use to both government and private sector entities. Private companies can use it for monitoring and safeguarding their events, while state agencies may assign the application to perform a variety of tasks, depending on their respective mandates.

Thus far, police authorities and other law enforcement agencies have been first to adopt the technology, with generally positive results. They have gradually accepted that information shared through social media can be crucial in their investigative and crime-prevention work. Signal's developers agree. They claim that the application enables authorities to:

1. respond to criminal activity
2. identify locations
3. identify potential witnesses
4. anticipate criminal activity
5. gather evidence including historic data
6. understand networks
7. identify social areas of interest

It also assists them in improving their reaction time to emergencies, and various incidents and threats, and in communicating more effectively with the general public.

A simple 3-step workflow is followed in operating the software:[22]

1. *Filter.* The user-entity decides what information it needs (i.e., location, topic, person, event, etc.) by building its search filters prior to the accumulation of information.
2. *Understand.* The information gathered is transformed into list and map formats in order to ensure "maximum information transfer with minimum effort".
3. *Integrate.* The real-time information produced is factored in when making strategic, tactical and operational decisions, ensuring "maximum possible situational awareness".

At present, the technology is reportedly used by the Royal Malaysian Police and a number of local police units in Australia and the U.S. It was in operation during the Cricket World Cup and Lindt Café Hostage Seige in Australia, as well as during Super Bowl LXIX and the Ferguson riots in the U.S.

[22] Signal, *Social Media Monitoring for Law Enforcement 2*.

Signal in the Philippines?

Documents disclosed to privacy advocates indicate that earlier this year, a meeting was held between the Philippine government and that of New Zealand, where the latter's representatives demonstrated Signal's surveillance and processing capabilities, particularly in filtering and harnessing social media data for purposes of intelligence gathering, threat identification, and real time investigation. Its use in addressing cybercrime and terrorism in the country was among those taken up in the ensuing discussions.

While the NZ government expressed its willingness to support a decision by the Philippines to procure the equipment, it remains unclear, if the two countries actually came into an agreement regarding such a transaction.

Remote Control System

The 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.[23] Classified as an intrusion technology, it operates in a manner that allows it to evade any encryption technology installed on that device. At the same time, its data collection remains undetected and its transmission of collected data to the RCS server is encrypted and untraceable. The following description of its features, as reproduced from an actual brochure, is instructive:

> Take control of your targets and monitor them regardless of encryption and mobility. It doesn't matter if you are after an Android phone or a Windows computer: you can monitor all the devices.
>
> Remote Control System is invisible to the user, evades antivirus and firewalls, and doesn't affect the devices' performance or battery life.
>
> Hack into your targets with the most advanced infection vectors available. Enter his wireless network and tackle tactical operations with ad-hoc equipment designed to operate while on the move.
>
> Keep an eye on all your targets and manage them remotely, all from a single screen. Be alerted on incoming relevant data and have meaningful events automatically highlighted.[24]

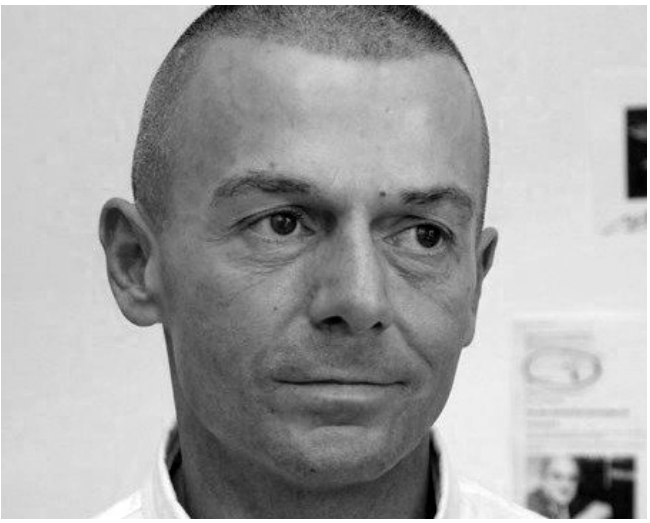
By contrast, PI was more succinct when it characterized the tool as "a suite of customised surveillance technologies designed to target electronic devices and allow the purchaser to copy files from a computer's hard disk, to record Skype calls, emails, instant messages and turn on a device's camera and microphone without the victim's knowledge".[25]

HackingTeam

RCS is the handiwork of HackingTeam, a firm of "50+ professionals" principally based in Milan, Italy, who focus exclusively on so-called "offensive security".[26] It claims to be the "world leader in providing state-of-the-art software tools for surveillance to law enforcement and intelligence agencies"[27] and boasts of the fact that its technology is "used daily to fight crime in six continents"[28].

[23] see: HackingTeam. *The Solution*, HACKINGTEAM, http://www.hackingteam.it/index.php/remote-control-system.
[24] HackingTeam. R*emote Control System Overview*. http://www.hackingteam.it/images/stories/galileo.pdf.
[25] Kenneth Page, *Did Hacking Team receive Italian public funding?*, PRIVACY INTERNATIONAL (Mar. 3, 2014), https://www.privacyinternational.org/?q=node/147.
[26] HackingTeam. *About Us*, HACKING TEAM, http://www.hackingteam.it/index.php/about-us.
[27] HackingTeam. *HackingTeam Complies With Wassenaar Arrangement Export Controls on Surveillance and Law Enforcement/Intelligence Gathering Tools*, HACKING TEAM (Feb. 25, 2015), http://www.hackingteam.it/index.php/about-us.
[28] HackingTeam. N 26.

Despite a report tracing its beginnings to 2001,[29] HT's own website states that the company was founded two years later, in 2003.[30] The following year, its proposal for an offensive solution for cyber investigations was supposedly so well-received that the company came to be venture backed by 2007.[31] According to an investigation conducted by PI, this infusion of funds amounting to €1.5 million originated from the Region of Lombardy, rendering the company's profits inherently intertwined with the public finances of a government entity.[32]



HackingTeam CEO, David Vincenzetti.
HACKINGTEAM 3
Source: http://static6.uk.businessinsider.com/image/55b22768371d2223518b8b2f-480/hacking-team-ceo-david-vincenzetti.jpeg

HT's clientele is a well-guarded secret. The company justifies this aversion to transparency by claiming that disclosure could "jeopardize ongoing law enforcement investigations".[33] Apparently, their clients need confidentiality when conducting surveillance of suspects involved in crime, terrorism or other illegal activity.[34]

In February 2014, however, Citizen Lab, a research institute based at the University of Toronto, released a report[35] identifying twenty-one (21) suspected former and current users of HT's RCS, namely: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan.

The Hack and Its Revelations

This year, the company itself fell victim to a major hacking attack, which led to 400GB worth of internal documents, source codes, and email communications being published online. This gave researchers, activists, and privacy advocates a rare look into the secretive world of the exploit development firm.

One interesting document from the leak was an invoice for €480,000, which seemed to come from the Sudanese national intelligence service.[36] HT has previously denied conducting business with Sudan. A separate document appeared to show the same country, along with Russia, listed as "not officially supported", as opposed to the "active" or "expired" status held by most other listed countries.[37] Not surprisingly, the list of HT clients revealed by Citizen Lab was essentially confirmed.

[29] Adrianne Jeffries, *Meet Hacking Team, the Company that helps the police hack you*, THE VERGE (Sep. 13, 2013), http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers.
[30] HackingTeam. *supra* note 26.
[31] id.
[32] Page, *supra* note 25.
[33] HackingTeam. *HackingTeam Response to Citizen Lab Report of March 9, 2015*, HACKING TEAM (Mar. 10, 2015), http://www.hackingteam.it/index.php/about-us.
[34] HackingTeam, N 33.
[35] Bill Marczak, et al, *Mapping Hacking Team's "Untraceable" Spyware*, CITIZENLAB (2014), https://citizenlab.org/wp-content/uploads/2015/03/Mapping-Hacking-Team%E2%80%99s-_Untraceable_-Spyware.pdf.
[36] Steve Ragan, *Hacking Team responds to data breach, issues public threats and denials*, CSO ONLINE (Jul. 6, 2015), http://www.csoonline.com/article/2944333/data-breach/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html.
[37] id.

One HT employee, Security engineer Christian Pozzi, initially took to Twitter to condemn the attack. He claimed that many of the data publicized were lies and dissuaded people from downloading the files as they were allegedly infected with a computer virus. He later deleted his account without explanation.

Although it is unclear who exactly was responsible for the hack, Motherboard tech website reported that a hacker named "PhineasFisher" has claimed credit.[38] The same individual hacked into Gamma International last year. Gamma, like HT, is also a developer of surveillance equipment.

Criticisms and Backlash

Even prior to the July attack, HT has been the subject of much criticism for its controversial products. Its business model—particularly its failure (or simple refusal) to control the sale of its spy tools to countries with poor human rights records—has been assailed by both activists and privacy rights advocates. In fact, in 2013, Reporters Without Borders named the company (along with Gamma) among the 5 "Corporate Enemies of the Internet," for selling products that are "liable to be used by governments to violate human rights and freedom of information".[39]

In PI's report, the descriptions of some of the company's major clients are nothing short of revealing:

> "…three of Hacking Team's clients – Uzbekistan, Saudi Arabia and Sudan – are ranked as "the worst of the worst" in terms of freedom, (sic) Freedom House's 2015 Freedom in the World index. Another three of the clients – Colombia, Mexico and Turkey – are on the Committee for the Protection of Journalists "20 Deadliest Countries" list in ranking attacks on journalists. Additionally, several of Hacking Team's clients have a history of human rights abuse linked to surveillance and intelligence technologies."[40]

[38] Lorenzo Franceschi-Bicchierai, *Hacker claims responsibility for the Hit on Hacking Team*, MOTHERBOARD (Jul. 6, 2015), http://motherboard.vice.com/read/hacker-claims-responsibility-for-the-hit-on-hacking-team.
[39] Reporters Without Borders. *Era of the Digital Mercenaries*. REPORTERS WITHOUT BORDERS, http://surveillance.rsf.org/en/.
[40] Page, *supra* note 25.

Despite the public outcry, HT has surprised many by managing to deflect widespread condemnation. It remains steadfast in its belief that its business is clothed with adequate legitimacy and propriety. A few weeks after its internal documents were leaked, HT published a statement on its website that listed down what it considered to be some fundamental truths regarding its work:

- "Hacking Team's technology has always been sold under the law. HT's surveillance tool has been provided only for the use of law enforcement, intelligence services and other government agencies, and never available to private individuals and businesses.
- Hacking Team does not conduct surveillance of suspects of crime, terrorism or other wrongdoing. That is the job of law enforcement.
- The attack on Hacking Team sometime before July 6 exposed much internal company data. However, since the data from investigations conducted by HT's law enforcement clients is stored on client computer systems, this surveillance data was not exposed in the attack.
- Today criminals can and do operate anonymously using encrypted digital tools such as modern email, mobile phones and portable computers. Every day criminals use these encrypted systems to sell drugs and sex, plot terrorist acts or even offer murder for hire.
- Law enforcement's ability to follow criminal activity is as important as ever, but today the job is enormously more complicated because of one simple reality: the secrecy of today's digital communications implemented in the name of privacy."[41]

RCS and the Philippines

While there are no confirmed reports of the actual existence—let alone, use—of the RCS in the Philippines, the leaked HT documents did reveal that a significant amount of interest was expressed by several parties purporting to represent different agencies of the Philippine government.

On 13 March 2011, an individual claiming to belong to the National Bureau of Investigation's (NBI) Cyber Center, working under of the Office of the Director, reached out to the company seeking a proposed solution to a potential "cyber attack offensive", similar to what was then a common occurrence in Australia.[42] In response to the query, HT outlined the salient features of the RCS.

[41] Hacking Team, N 26.
[42] WIKILEAKS, https://wikileaks.org/hackingteam/emails/emailid/605081

In January 2013, an individual named "Gadburt Mercado" began communicating with Daniel Maglietta, Chief of HT's Singapore Representative Office, to set up a product demonstration meeting between HT executives and Mr. Mercado's supposed principal, Col. Manuel Lucban, Chief of Police of Makati City. Spanning a period of more than a year, the email thread suggests that no actual meeting took place during such time due to the conflicting schedules of the parties.[43]

As recent as March 23 of this year, a person claiming to be an officer of the Intelligence Services of the Armed Forces of the Philippines (ISAFP) relayed his unit's interest in the capabilities of HT's Galileo Remote Control System.[44] He requested for additional information from the company, as well as a product demonstration. As in the case of Mr. Mercado, seems there was also a failure in the negotiations, albeit, this time, it was due to a shift in focus by the ISAFP towards other projects and capabilities.[45]

HT is also regularly invited to PROTECT, a local government-private sector-initiated conference and exhibition series on security and safety.[46] Launched in 2005 by Leverage International (Consultants), Inc.,[47] in cooperation with the Anti-Terrorism Council, this year's event was held last March 23 and 24, and featured panel discussions on issues like regional and global terrorism and radicalization, cyber security and data protection, transnational crimes, chemical, biological, radiological and nuclear (CBRN) defense, and brand protection. The exhibit included network security services for computing infrastructures, emergency lighting and security, biometrics services, building automation and electronic security systems, mobile asset tracking, and interestingly enough, advanced surveillance and access control systems. The HT leak suggests that the company opted not to attend this year.[48] It is unclear if it has graced any of the event's previous editions.

[43] WIKILEAKS, https://wikileaks.org/hackingteam/emails/emailid/17209
[44] WIKILEAKS, https://wikileaks.org/hackingteam/emails/emailid/17032.
[45] WIKILEAKS, https://wikileaks.org/hackingteam/emails/emailid/17032.
[46] Leverage International, *Quick Facts*, LEVERAGE INTERNATIONAL, http://www.protect.leverageinternational.com/quick-facts.html.
[47] *see:* Leverage International, *The Company*, LEVERAGE INTERNATIONAL, http://www.protect.leverageinternational.com/company.html.
[48] WIKILEAKS, https://wikileaks.org/hackingteam/emails/emailid/351946.

"Spectrum"

On 7 April 2014, news of an acquisition by the Philippine government of a Php135M ($3.4M) surveillance equipment surfaced.[49] Supposedly covered by a 26 October 2011 purchase request,[50] the device was described as a "Radio Frequency Test Equipment" (RFTE) that went only by the name, "Spectrum," in the relevant government records. The vendor was identified as Rohde & Schwarz (R&S), an electronic surveillance company based in Germany.[51]

The report went on to describe the "Spectrum" portfolio as consisting of "portable analyzers and handheld monitoring receivers for the general purpose of signal investigation and scalar networking."[52] However, as regards the equipment actually purchased, the news source pointed out its ability to collect massive amounts of information from such varied sources as emails, social media posts, text messages, and cellphones. In a later report, the gadget would also be described as customizable allowing for the monitoring of distant radio frequencies "running on certain protocols such as phones, handheld radios, and wi-fi devices, and anything that produces radio frequencies."[53] Apparently, it is resistant to existing counter-surveillance technology, with even the most modern scramblers unable to impair its effectiveness.

Delivery of the equipment was allegedly made in November 2013, with the unit already being set up at the ISAFP Headquarters in Camp Aguinaldo at the time of the report. Full operational capacity was expected sometime between June and August 2014.

The exposé also claimed that, once in use, the primary purpose of the tool was to spy on critics of the administration, including their families and minor children. It was supposed to give the Aquino government a key advantage in the incoming 2016 Presidential elections.

Rohde & Schwarz

Rohde & Schwarz (Philippines), Inc. describes its business as meeting "the fast-paced demands of Test & Measurement, Communications, Broadcasting, Radio Monitoring and Radiolocations in the Philippines".[54]

[49] Tribune Wires, *P135-M spy gadgets trained on opponents*, TRIBUNE (Apr. 7, 2014), http://www.tribune.net.ph/headlines/p135-m-spy-gadgets-trained-on-opponents.
[50] Special Allotment Release Order No. D-11-024613.
[51] Tribune Wires, *supra* note 49.
[52] id.
[53] Charlie V. Manalo. *RP now a 'Big Brother' state* – UNA, TRIBUNE (Apr. 12, 2014), http://www.tribune.net.ph/headlines/rp-now-a-big-brother-state-una.
[54] Rohde & Schwarz, *About R&S Philippines*, ROHDE & SCHWARZ, http://www.rohde-schwarz.com.ph/en/About_R%26S_Philippines/.

Established in July 2003, it currently maintains its office in Makati City, while R&S—its mother company—is headquartered in Munich, Germany. Last December 2014, the company supplied the government with voice over IP (VoIP) technology for air traffic control (ATC).[55] R&S is also part-owner of Portuguese military communications company, EID, which was recently contracted to deliver a complete integrated communications system for two strategic sealift vessels (SSVs) on order for the Philippine Navy (PN).[56]

While most publicly available information regarding R&S's product range do not suggest significant company focus on surveillance equipment or capabilities, accounts of its activities in this area do exist.

For one, the company claims to have produced the first commercial version of IMSI catchers when it filed a patent registration application in 2003.[57] IMSI catchers refer to "a class of devices that emulate cell towers in order to capture the International Mobile Subscriber Identification (IMSI) number of cell phones".[58] Acting as a fake base station tower in mobile networks, it works by sending out a stronger signal than a nearby mobile network tower. When cell phone SIM cards check in with the tower, the device begins snatching the IMSIs of all mobile devices within range, without identifying itself to the targets[59] or to the unsuspecting wireless service provider whose network is being spoofed. It is able to log all incoming calls, including, in most cases, the contents thereof. Today, some systems can even activate video cameras or trigger malwares that take over the target's device.

ROHDE AND SCHWARZ 1
Source: https://cdn.rohde-schwarz.com/pws/general/cws/about/about_01.jpg

[55] Rohde & Schwarz GmbH & Co. KG, *Philippine Department of Transportation and Communications (DOTC) migrates ATC toward VoIP with Rohde & Schwarz technology*, NOODLS (Dec. 16, 2014), http://www.noodls.com/view/416D58EFDBFB1BE0D42276E0FD2166E553281181?1812xxx1418839515.
[56] Victor Barreira, *Portugal's EID to supply communications systems for Philippine sealift ships*, JANES (May 12, 2015), http://www.janes.com/article/51406/portugal-s-eid-to-supply-communications-systems-for-philippine-sealift-ships.
[57] *Is Harris Stingray Above the Law?*, INSIDE SURVEILLANCE (Jan. 6, 2015), https://insidersurveillance.com/harris-stingray-law/.
[58] *Is Harris Stingray Above the Law?*, N 57.
[59] Originally designed to capture the IMSIs of GSMs devices, IMSI catchers now work with any type of mobile device.

With such intrusive technologies forming part of its portfolio, controversy has followed the company in recent years. In March 2006, for example, a German TV program reported on exports made by R&S to Uzbekistan involving a "system for the surveillance of radio frequencies" that can also monitor mobile phone calls.[60] The country is notorious for state-sponsored abuses and the torture of prisoners.[61]

Government Response

Despite its incredible and largely unsubstantiated claims, the local report managed to gain traction in local news owing to the inconsistent (and ambiguous) statements made by various government officials.

The day after the report came out, ISAFP Chief Maj. Gen. Eduardo Año vehemently denied that his unit had acquired any high-end surveillance equipment.[62] He insisted that the ISAFP is a professional organization focused on gathering intelligence against threats to national security and terrorist groups and not for any political purpose.

Meanwhile, Deputy Presidential Spokesperson Abigail Valte was more cryptic in her response when asked about the veracity of the report. She maintained that under no circumstances had the Aquino administration carried out spy work against perceived political opponents, critics, or journalists. The President, she added, always made sure that government assets are used properly and/or for correct purposes.

A day later, the Department of National Defense set aside Valte's statements when it confirmed the acquisition of "spy gadgets". It pointed out, however, that there was nothing unusual with the acquisition of an RFTE, given that it was part of the capability upgrade efforts of the Armed Forces of the Philippines (AFP) and was meant to boost the latter's capacity to "combat terrorism and protect the Filipino nation and its people".[63] The Department also cited the country's primary anti-terror law (Human Security Act of 2007) as a tenable legal justification. Nevertheless, it stood firm in asserting that the gadgets were not meant for politically-motivated missions or unwarranted intrusions into the people's right to privacy. It also denied the existence of a State-sponsored project called "Spectrum".

Presidential Spokesperson Herminio Coloma later affirmed the DND's position when he, too, admitted the purchase of spy tools and characterized the same as part of the AFP Modernization Program.

[60] *Surveillance*, GERMAN FOREIGN POLICY (Apr. 16, 2008), http://www.german-foreign-policy.com/en/fulltext/56148/print?PHPSESSID=bvlheko5it2kvr1qlgr291mmc2.
[61] id.
[62] Mario J. Mallari, *ISAFP WON'T ENGAGE IN POLITICS THROUGH SPYWARE*—INTEL CHIEF, TRIBUNE (Apr. 8, 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.
[63] Tribune Wires, *Noy dares critics: Prove spy tools' use vs political foes*, TRIBUNE (Apr. 11, 2014), http://www.tribune.net.ph/headlines/noy-dares-critics-prove-spy-tools-use-vs-political-foes.

He explained that the equipment would be used in the campaign against terrorism, similar to those operated by the U.S. He also dared critics to substantiate their claim that the tools would be used against President Aquino's political enemies and critics.

"Outrage"

Presented with an opportunity, main opposition party, United Nationalist Alliance (UNA), latched on to the issue and moved quickly to condemn the mysterious government transaction. Three days after the story broke, the group came out to corroborate the "elaborate spying operation" the Aquino administration was supposedly planning against opposition forces.[64] UNA Secretary General, Navotas Rep. Toby Tiangco, said that the party had received "credible information" confirming that the equipment acquired by the government is similar to that used by U.S. authorities in counter-terrorism operations, and that it will be used to spy on civilians, particularly those critical of the administration. He clarified, however, that based on their information, a different intelligence agency (and not the ISAFP) was going to operate the new equipment.

The next day, the newspaper that first came out with the report emphasized anew its earlier statement that journalist-critics of the administration were already aware that their phone conversations were constantly under surveillance, even prior to the recent purchase of spying equipment.[65]

It followed this up with another article on 12 April 2014, where it made reference to George Orwell's Big Brother concept and declared unequivocally that the Philippines "is now living under a surveillance state".[56] It added that "even elected senators have already noted that their phone conversations are being bugged with their phones even being triangulated for easy tracking".[57] The paper also cited Tiangco who was then accusing the administration of "conveniently invoking its authority to spy on civilians" pursuant to the Human Security Act.

This year, on 23 April 2015, UNA, through its interim secretary general, JV Bautista, found a chance to revisit the PhP135 million purchase when it questioned the possible use by Sen. Antonio Trillanes IV—a known critic of Vice President and UNA standard-bearer, Jejomar Binay, Sr.—of Development Acceleration Program (DAP) funds for the purchase of spy equipment.[68] In accusing the Senator of failing account for much of the PhP245M DAP funds released for his projects, UNA cited the "Spectrum" purchase and suggested a possible connection to the Senator's expenditures and accounting woes.

[64] Charlie V. Manalo. *UNA affirms P135-M spy devices vs. Noy critics*, TRIBUNE (Apr. 10, 2014), http://www.tribune.net.ph/headlines/una-affirms-p135-m-spy-devices-vs-noy-critics.
[65] Tribune Wires, *supra* note 63.
[66] Charlie V. Manalo. *supra* note 53.
[67] id.
[68] Charlie V. Manalo. *Trillanes may have used DAP funds for s'special missions'* – UNA, TRIBUNE (Apr. 23, 2015), http://www.tribune.net.ph/headlines/trillanes-may-have-used-dap-funds-for-special-missions-una.