GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

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

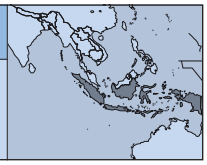
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

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

INDONESIA

Taming the untameable: Indonesia's effort to control the growing tide of digital communications



Anonymous
Anonymous

Introduction

Following three decades of a restrictive Suharto-led government characterised by "political repression and ideological surveillance,"[1] Indonesia has morphed into a relatively open society with more democratic space. Along with this openness, it has witnessed a massive transformation in the area of information and communications technologies (ICTs). Indonesia has the fourth largest mobile phone market in the world with 278 million subscribers.[2] By 2015, it is expected that nearly 115 million will have access to the internet.[3] The country has been hailed by civil society activists as "regional champion for freedom of expression."[4] Indonesia's capital, Jakarta, is called the "social media capital of the world" with more tweets coming from the city than any other capital in the world.[5] It is the only country in the region to provide protection of free speech through a legal framework called the Transparency of Public Information Law, which guarantees access to state information, and the Press Law, which protects journalistic work as "an important component of [...] free speech and access to information."[6]

At the same time, legal frameworks continue to tightly limit basic freedoms, justified by arguments concerning traditional values or the maintenance of national security. This is demonstrated through notable legal setbacks, such as the Mass Organisation Law that restricts the right to freedom of association. The Intelligence Law of 2011 enforces further restrictions by allowing the security apparatus "significant latitude in intelligence gathering aimed at 'opponents' of 'national stability'."[7]

The country's first and only cyber law, the Electronic Information and Transaction Law, prohibits the publishing of content to do with gambling, and defamation and threats. The Indonesian parliament has also passed an Anti-pornography Law, which is routinely used to block LGBT (lesbian, gay, bisexual and transgender) content on the internet.[8] In addition, the country has also adopted a number of laws that prohibit defamation of religion, which is used broadly to block content that provides alternative views on Islam, the religion of the majority of Indonesians.

While the boundaries of expression have widened notably, and are more open generally in Indonesia than in its regional counterparts, the country is a mixed picture of freedom of expression. As suggested, norms of expression are reinforced through a variety of anti-pornographic, anti-blasphemy and anti-defamation laws. In legal terms and in practice, Indonesia has also regularly demonstrated that "national security" or "national stability" interests trump freedom of expression. While censorship is overt, surveillance is less visible but also pervasive, with each carried out by different government agencies.

This report looks at communications surveillance in Indonesia by examining the recent purchases of sophisticated surveillance equipment by the military. It opens up questions about the potential use of this new equipment and what this means for freedom of expression in the country.

Surveillance +

In the book *Democratisation of Post-Suharto Indonesia*, Jun Honna argues that "political repression and ideological surveillance were the major tools used" by Suharto to remain in power.[9] These "politico-ideological" surveillance tactics were carried out principally by the military, targeting journalists,

1 Bünte, M., & Ufen, A. (eds.) (2009). *Democratisation in Post-Suharto Indonesia*. Oxford: Routledge.

2 Indonesia's population is 247 million. Due to multiple phone subscriptions, this number of mobile subscribers is higher than the population. www.redwing-asia.com/market-data/market-data-telecoms

3 www.slideshare.net/OnDevice/indonesia-the-social-media-capital-of-the-world

4 Southeast Asian Press Alliance. (2013, July 8). Indonesia's Ormas Law: A ready weapon against civil society and free speech. IFEX. https://ifex.org/indonesia/2013/07/08/ormas_law

5 www.slideshare.net/OnDevice/indonesia-the-social-media-capital-of-the-world

6 Southeast Asian Press Alliance. (2013, July 8). Op. cit.

7 Ibid.

8 Citizen Lab and Canada Centre for Global Security Studies. (2014). Islands of Control, Islands of Resistance: Monitoring the 2013 Indonesian IGF. www.citizenlab.org/briefs/29-igf-indonesia/29-igf-indonesia.pdf

9 Bünte, M., & Ufen, A. (eds.) (2009). Op. cit., p 230.

students, intellectuals and activists, essentially muzzling dissenting voices in the country. While a relatively free media and civil society activism have flourished in the wake of Suharto's removal, the practice of military surveillance continues. The Indonesian military continues to project a role as the protector of national unity, and to demarcate the limits of political and ideological expression in the country through a range of practices, including surveillance.

Complementing its traditional intelligence collecting approaches, and in parallel with the massive growth of internet use, the military is expanding its online surveillance capability. In January 2013, the *Jakarta Globe* reported that Indonesia's Ministry of Defence purchased GBP 4.2 million (USD 6.7million) worth of surveillance products from Gamma Group, a UK-based company that provides sophisticated surveillance equipment to governments.[10] While the exact type of product procured was not disclosed, Gamma Group sells products ranging from mobile surveillance vans to software like FinFisher, which is capable of monitoring all internet communication in the country.

In fact, FinFisher command and control servers were already found to be at work in Indonesia in 2012. According to a report released by Citizen Lab in 2012, FinFisher products were found on several Indonesian internet service providers (ISPs).[11] The Indonesian government has not publicly stated if it is the one deploying this intrusive software or clarified its intended use. Gamma Group, on the other hand, has stated that it only provides services to governments and not private individuals and companies. Based on these statements, one can surmise that complex communication surveillance machinery is in place in Indonesia, and its use only seems to be expanding over time.

Rights activists are concerned about the implications of these findings. "I'm afraid there're not enough mechanisms and self-control to ensure that this technology is not abused," Andreas Harsono, Indonesia researcher with Human Rights Watch, told the *Jakarta Globe*. "Indonesia has no third-party intelligence gathering mechanism – be [it] a court or a legislative mechanism – to approve wiretapping. The Gamma equipment is a nightmare."[12]

The Intelligence Law is applied to intelligence gathering activities in Indonesia. When an updated version of the law was passed in 2011, rights groups criticised it for its expansive scope and its vague wording, which allows for "significant intelligence gathering over opponents of national stability."[13]

The government has referred to terrorism, including two bombings in Bali in 2002 and 2005, as well as multiple attacks in Jakarta, as justification for surveillance. While the government has said surveillance products will be used "only for strategic intelligence,"[14] rights groups and activists have warned that it could be used to monitor, and potentially silence, civil society and media.

The current situation in West Papua illustrates the broad application of the government's definition of "opponents of national stability". West Papua[15] is the easternmost province of Indonesia with a large presence of the military's Special Forces to combat the Papuan separatist movement, the Free Papua Movement (*Organisasi Papua Merdeka* or OPM), who have been engaged in armed resistance. International media are blocked from entering the province and international organisations have been prevented from operating in the region.

In 2011, a report by Human Rights Watch, citing internal military documents, asserted that military surveillance in the province monitored not only the OPM, but a "broad swathe of Papuan political, traditional, and religious leaders and civil society groups."[16] This surveillance was carried out entirely without "judicial warrant and without clear evidence of wrongdoing."[17] The internal documents also showed that the intention of the government was to prevent the free flow of information to and from Papua. According to one document: "Current political activity [e.g. by civil society and students] in Papua is very dangerous compared to the activities of Papuan armed groups, because [civil society] influence already reaches abroad."[18]

Physical surveillance and rudimentary surveillance tactics are well known by Papuan activists and journalists. An Indonesian journalist who wished to remain anonymous stated in an interview that phone tapping is common. "When you are in Papua and if you are calling someone, you can hear other people talking. It is called crossed lines, when it is accidental. In Papua, every call you make is like

10 Vit, J. (2013, September 25). TNI surveillance purchase triggers concern in Indonesia. Jakarta Globe. www.thejakartaglobe.com/news/tni-surveillance-purchase-triggers-concern-in-indonesia

11 Citizen Lab and Canada Centre for Global Security Studies. (2014). Op. cit.

12 Vit, J. (2013, September 25). Op. cit.

13 Southeast Asian Press Alliance. (2013, July 8). Op. cit.

14 Vit, J. (2013, September 25). Op. cit.

15 Now divided into Papua and West Papua.

16 Human Rights Watch. (2011, August 14). Indonesia: Military documents reveal unlawful spying in Papua. Human Rights Watch. www.hrw.org/news/2011/08/14/indonesia-military-documents-reveal-unlawful-spying-papua

17 Vit, J. (2013, September 25). Op. cit.

18 Human Rights Watch. (2011, August 14). Op. cit.

that."[19] Intelligence agencies have even set up phone charging booths to collect phone numbers. "When you charge your phone, you have to give them your number. There is evidence of intelligence agencies using phone credit stores to supply numbers to the military. Usually these are targeted at NGOs."

Papuan journalists and activists say surveillance extends to other forms of communication. "Many times, I have received notification from Gmail that someone tried to access my account," said Latifah Anum Siregar, head of the Alliance for Democracy for Papua (*Aliansi Demokrasi untuk Papua*).[20] "Our website adlp-papua.com has been hacked several times. When that happens data is usually missing, files cannot be downloaded."

"In the past three years, our website tabloid-jobi.com has been hacked six times. We are also aware of surveillance on the internet," said Victor Mambor, head of the Alliance of Independent Journalists in Papua.[21] "Our Twitter and Facebook are being monitored." Journalists often receive calls and orders from the military asking them to hand over tapes and other recordings, especially if they are covering events relating to political dissent, like demonstrations, Mambor said.

Papuan activists interviewed for this report have also spoken of the practice of self-censorship on social media sites over fears of being physically harmed by security forces. "Now I only trust face-to-face communication. I rarely use the telephone to talk about sensitive issues."

Even without surveillance, Indonesia has demonstrated a position of not fully supporting freedom of expression on the internet. With a variety of anti-pornographic, anti-defamation and anti-rumour mongering laws, it already blocks content on the internet. As suggested, this has been manifested in blocking content that discusses LGBT rights and content that provides alternative views on religion.

The silencing of local voices from Papua is not limited to strictly political expression. In March 2014, a live video-cast of two Papuan tribesmen speaking at a major environmental conference in the United States was disrupted by an online attack on the site, which rights activists say came from parties linked to the Indonesian government.[22]

19 Interview with an anonymous journalist on 23 May 2014.

20 Interview with Latifah Anum Siregar, head of the Alliance for Democracy for Papua, on 3 June 2014.

21 Interview with Victor Mambor, head of the Alliance of Independent Journalists in Papua, on 3 June 2014.

22 Sloan, A. (2014, March 20). Indonesia suspected of hacking to silence abuse allegations. Index on Censorship. www.indexoncensorship.org/2014/03/indonesia-suspected-hacking-silence-abuse-allegations

Opportunities for reform?

There are indications that a multi-pronged surveillance system, employing sophisticated software and taking advantage of weak legal protections for expression, will mean that it will be even easier to suppress freedom of expression on the internet in the future.

There are some potential opportunities that could be leveraged for reform. The Indonesian government hosted the annual global Internet Governance Forum (IGF) in Bali in 2013, which opens up a space for debate surrounding freedom of expression on the internet. The timing of the IGF, directly following the Snowden revelations, raised the profile of surveillance at the forum.

In the immediate future, whether this trend towards openness continues will be influenced by which candidate wins the presidential elections in July 2014. The candidates for president, Prabowo Subianto and Joko Widodo, appear to maintain starkly different positions on these issues. Prabowo is taking a hard-line nationalistic stance that could mean setbacks in terms of rights of expression, as he would appear to be less tolerant of dissent, while Jokowi, as he is known, is campaigning on a platform of transparency.

In the meantime, journalists and activists continue to tolerate limits to their freedom. "I accept this surveillance as the risk of my job. There is nothing we can do except to accept this as part of our everyday reality," said Mambor. "People in Jakarta may have choices, but we, in Papua, don't. There is only one internet provider and the service is not good."

Siregar further echoes this sentiment, stating, "I tell my colleagues that our job is full of risks. Don't expect that our name is not already recorded by the intelligence [agencies] and our picture and data isn't in their system already."

Action steps

Based on the current scenario, the following action steps are recommended for activists and journalists:

- Be aware of the prevalence of surveillance, and take protective measures when communicating online by using secure tools.
- Make your colleagues and associates aware of surveillance; teach them to use secure methods of communications.
- Engage with freedom of expression activists locally and internationally to leverage change in this area.
- Lobby governments for stronger legal protections around freedom of expression.