



A question of trust: Myanmar's shadowy world of digital surveillance

DECEMBER 20, 2015



People in Myanmar are more connected than ever and, with a record behind every call and text, easier than ever to track.

By JAMES COE | FRONTIER

“They always followed me; every day, every night,” said Ashin Gambira over the crackling of an intermittent Skype connection, “but I am safe now.” Ashin Gambira has been living in self-imposed exile in Thailand since 2013 after serving more than four years in prison for his leading role in the 2007 monk-led protests known as the Saffron Revolution.

He is no stranger to the panoptical effect of government surveillance. “[During the revolution] I used two satellite phones, one from Thailand and one from Singapore so the government could not listen to my calls.” Despite his best efforts to evade the authorities in the brutal crackdown that followed the protests, Ashin Gambira was eventually arrested and sentenced to 68 years in prison. He was released under a presidential pardon in early 2012 but was arrested at least three times in the following 11 months before leaving the country.

“I still don’t trust the Burmese government,” said Ashin Gambira, whose health suffered as a result of being tortured in prison. “After the transfer of power there will be many political problems; the problems will continue but with the new [National League for Democracy] government, it will get better.”



On the issue of surveillance, however, he is less optimistic. He is concerned that the Ministry of Home Affairs will remain under military control and the surveillance of political activists will continue. It was a problem an NLD government would not be able to solve, he said, adding that the military did not trust the people.

“They are afraid of the people because they have made a lot of problems for them for 50 years.”

Support independent journalism in Myanmar

[Sign up to be a Frontier member.](#)

Access to mobile technology in Myanmar has boomed in recent years, and there are more than 35 million active SIM cards in the country. Many users will be unaware that every call, text message, email they send and website they visit, open or visit leaves a record. The location of cellphone users can be triangulated to within 2,000 feet (about 610 metres); a smartphone user can be pinpointed to within 27 feet (about 8 metres).

Much of the modern world is still wrestling with how much data is stored, who has access to it and what oversight powers should be in place. As Myanmar rapidly modernises, and its citizens begin to generate vast amounts of data, it must swiftly decide where to draw the line between security and privacy.

“Physical and communication surveillance concerns have been on-going in Myanmar for decades ... Whilst the full extent and scope of its communication surveillance capabilities remain unclear, there is evidence of Myanmar having purchased surveillance technologies,” Alexandrine Pirlot de Corbion of London-based watchdog Privacy International told Frontier.

The sale of surveillance technology is notoriously secretive and it is often difficult to find out what capabilities a government is trying to obtain. However, earlier this year Wikileaks offered a glimpse into the situation in Myanmar when it released a trove of confidential emails from Hacking Team, an Italian-based technology company that specialises in offensive intrusion and surveillance capabilities. The cache included emails showing that the Myanmar government had approached the company about buying its equipment.

Hacking Team’s products enable governments to monitor communications, decipher encrypted files and emails, remotely activate microphones and cameras, record Skype calls and intercept VoIP calls such as those made on Viber.

One of the emails released by Wikileaks was sent to Hacking Team by U Aung Lynn Thway of Naung Yoe Technologies in 2014.

“We got your contact from ISS World Training in Czech where we visited with two colonels from [the] Ministry of Defence, Myanmar,” wrote Aung Lynn Thway. “MoD is interested in your offensive solution on mobile devices and request us to contact HT [Hacking Team] on behalf of them.” [sic]

The next month, Daniel Maglietta, the chief of Hacking Team’s Singapore representative office wrote in an internal email: “I was wondering if you had any particular updates about the offer we sent to Myanmar [?]”

It is not known what the offer was or if it was accepted by the Myanmar government.

“Physical and communication surveillance concerns have been on-going in Myanmar for decades ... Whilst the full extent and scope of its communication surveillance capabilities remain unclear, there is evidence of Myanmar having purchased surveillance technologies.”

“We know that Myanmar was a surveillance state for a long time, and this was before Myanmar had the connectivity and technology it has now and will have in the future,” said Lucy Purdon, from the Institute for Business and Human Rights, a think tank in London. “As Myanmar does not yet have rules governing surveillance in place, the use of this technology would be very concerning as the surveillance powers would be limitless,” Ms Purdon said.



“If they [the government] hack their [citizens’] stuff, it’s illegal; they won’t get that information from me,” said Telenor’s chief corporate affairs officer, Gunnar Bertelsen. “If you are looking at the social activist in Kachin [who has been arrested for defamation], for instance, on Facebook – that has nothing to do with the operators,” said Mr Bertelsen, referring to U Patrick Khum Jaa Lee, who is on trial for breaching Section 66(d) of the Telecommunications Law over a Facebook post he allegedly shared showing a doctored image of Tatmadaw Commander-in-Chief Senior General Min Aung Hlaing.

However, there are more transparent and legitimate uses of surveillance tools, including providing telecommunications data to assist criminal investigations.

Under the Telecommunication Law, operators are obliged to store their customer’s communications data. Article 69 of the Law stipulates that the government must obtain a court order for the disclosure of this information. However, the law governing the interception of communications by law enforcement authorities is yet to be drafted.

To obtain access to an individual’s data, the police must file a “first instance report” with a magistrate and if a court order is granted, the request will also go to the Posts and Telecommunications Department and the Home Affairs Ministry in Nay Pyi Taw. If the request is approved a recommendation is sent to the telecommunications company, which decides whether or not to release the data. “We have to verify that it holds up, as such, that it is a genuine serious crime issue,” said Mr Bertelsen.

It is unusual for a private company anywhere to be able to overrule decisions made by courts and government agencies but the procedure in Myanmar is helping to prevent undue intrusion.

“Old habits die hard,” Mr Bertelsen said. “I frequently say no [to requests for data] ... the crime itself might not warrant the intrusion of the release of that data,” he said.

“You have to remember that before we [Telenor] came in [2014], the government would get any kind of information from the state-owned operator on this, so there was no vetting as such ... previously, there was nothing but that has to be seen in the context of the type of country it was at the time ... it’s a learning curve for them [the government] as well.”

Telenor stores call data records for 18 months, including the location of the cell tower most recently used by a customer. It does not store the content of communications and is only able to locate users to within a “couple of square kilometres,” said Mr Bertelsen.

Telecommunications providers are able to maintain the relatively low levels of customer’s data they keep and reject court-ordered requests for information about customers because there is a lack of legislation compelling them to do otherwise. That is likely to change. Draft legislation is due to be released for public consultation in the first half of next year. “It’s extremely important that civil society gets involved and sets the framework,” said Mr Bertelsen.

In the realms of surveillance, the growth of telecommunications in Myanmar has outpaced its political and legislative process. As the next parliament catches up a key element of the debate will be the right to privacy. Meanwhile, people’s privacy hinges on trust. Trust that the government has not bought powerful and intrusive software; trust that the courts will not rubber-stamp government requests for data; and trust that telecommunications providers will act as a final barrier to unsubstantiated requests.

Title photo: Ann Wang / Frontier

More stories





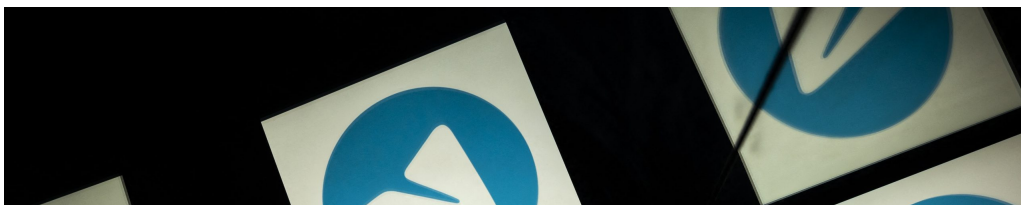
‘Watermelon suppression’: doxing campaign targets pro-democracy soldiers and police

Military-linked social media accounts, mainly on Telegram, continue to dox activists and encourage violence, including assassinations. Although one of the most controversial accounts was recently removed from the platform, critics say Telegram is still not doing enough to regulate content.

Related stories



The online activists helping Myanmar troops desert





Channelling hate and disinformation: Myanmar’s bad actors move to Telegram



Stay or go? Telenor’s Myanmar dilemma

Latest Issue





VOLUME 6, ISSUE 18 JANUARY 27, 2021

STORIES IN THIS ISSUE

Myanmar enters 2021 with more friends than foes

The early delivery of vaccines is one of the many boons of the country's geopolitics, but to really take advantage, Myanmar must bury the legacy of its isolationist past.

Will the Kayin BGF go quietly?

The Kayin State Border Guard Force has come under intense pressure from the Tatmadaw over its extensive, controversial business interests and there's concern the ultimatum could trigger fresh hostilities in one of the country's most war-torn areas.

SUBSCRIBE

VIEW ALL ISSUES

BECOME A FRONTIER MEMBER

Support our independent journalism and get exclusive behind-the-scenes content and analysis

JOIN US

GET EXCLUSIVE DAILY UPDATES

Stay on top of Myanmar current affairs with our Daily Briefing and Media Monitor newsletters.

SUBSCRIBE



JOIN THE COMMUNITY

Sign up for our Frontier Fridays newsletter. It's a free weekly round-up featuring the most important events shaping Myanmar

Your email address

SIGN UP



- MAGAZINE
- MEMBERSHIP
- THE FRONTIER STORY
- WORK WITH US
- DONATE
- CONTACT US

FOLLOW FRONTIER



LANGUAGE
ENG BUR

© 2020 FRONTIER MYANMAR

PRIVACY POLICY

