



Youths browse Facebook at a Yangon cybercafe on December 18, 2018. (AFP)

Junta steps up phone, internet surveillance – with help from MPT and Mytel

JULY 5, 2021



A police cybersecurity team is working with state- and military-owned mobile operators to monitor phone users in real time, and to identify and track regime opponents online.

By FRONTIER

Before February 1, activist Ma Myat Su Mon didn't give much thought to digital security. She used a SIM from military-linked mobile operator Mytel, spoke openly on phone calls and sent unencrypted messages using Facebook Messenger.

Since the coup, Myat Su Mon has emerged as a protest leader in the town of Kalay in Sagaing Region, where opposition to military rule has been particularly fierce. The junta's brutal suppression of the protests forced her into hiding, and suddenly digital security was a life-or-death matter.

"I'll never use my Mytel SIM again because I don't trust them. I'm using Telenor and Ooredoo and I feel more secure," she told *Frontier* in a recent interview, referring to Myanmar's two foreign mobile operators.

Even so, she doesn't speak openly on the phone anymore; like many people, she suspects the authorities are monitoring her calls. When she needs to communicate with her fellow activists, she uses the encrypted messaging app Telegram, and is always careful to use a virtual private network, or VPN.

"No one trusts them [the military] – we have to be very careful about our safety," she said. "As long as we can access the internet, we don't talk on the phone. If we need to use the phone, we use Telenor or Ooredoo SIM cards and don't mention any places, our plans or our real names."



Call monitoring

These concerns are not misplaced. Late last year, shortly before the coup, the Ministry of Transport and Communications directed the Myanmar Police Force to set up a cybersecurity team to monitor calls and social media use, a police officer on the team told *Frontier*, speaking on condition of anonymity.

The team is based inside the police's Special Branch, whose plain-clothed officers are well known for their intrusive surveillance of the population, and the team's activities complement the specific case work of the Criminal Investigation Department's Cybercrime Division.

Although initiated under the National League for Democracy government, the monitoring has become key to the new military regime's efforts to establish what some have described as a “[surveillance state](#)”, in which authorities closely track phone and internet use and seize devices from ordinary civilians before analysing them for incriminating material.

The new team began its work around a month after the coup, when the ministry introduced what the police officer described as an “AI system” that enabled the team to monitor the calls, text messages and location of selected users in real time.

If specific words, such as “protest” or “revolution”, are mentioned during the call, then the system automatically records it. It also triggers a notification for police so the call can be reviewed and, if necessary, the user can be placed under heavier surveillance or the call retained as evidence.

Known as “lawful interception”, this real-time monitoring marks a major increase in surveillance of phone users that experts say is concerning in a context like Myanmar, where there are few legal safeguards.

Previously, security forces could only access historical data from users – for example, who they had called and their location based on which cell tower they had connected to – by making a request to the relevant operator.

The officer did not know how many users were being monitored, but said it was a significant number. “We can't monitor all conversations so they need a system that just flags sensitive calls. It's not a particularly advanced system but it works well for now,” he said.

A little help from our friends

The police officer said that the programme had not yet been rolled out to all operators and ISPs, including foreign-owned mobile operators Telenor and Ooredoo.

Among mobile firms, only Mytel – whose investors include the Tatmadaw, a consortium of Myanmar companies and Viettel, a company owned by the Vietnamese military – and state-owned MPT, which is run under a partnership with Japan's Sumitomo and KDDI, have installed the system at their data centres, he said.

He was speaking prior to a Reuters [report](#) that the junta had banned foreign and Myanmar executives of “major telecommunications firms” from leaving the country without permission. A week after the ban was announced in mid-June, the operators received another order instructing them to install intercept technology by July 5 that would let the regime spy on their customers. It is unclear whether they have complied.

A senior executive at one of the foreign operators told *Frontier*: “The technical term is lawful interception, and the [authorities have] been pushing for this for some time – it started under the NLD. We have not implemented this, but I am pretty sure other operators are running it.”

Recent changes to the Electronic Transactions Law grant the authorities almost unlimited access to user data without even basic safeguards.

Free Expression Myanmar, an advocacy group, said that under the February 15 amendment there are no limitations on the type or scale of the data that can be intercepted, and no clarity on how intercepted data should be handled, or for how long. The amendment “represents a significant risk to civic space” it said, adding that the regime now has “broad powers of interception without even the most basic safeguards for misuse”.

A senior official from MPT told *Frontier* that the company was not only providing user data to the cybersecurity team but had also dramatically stepped up surveillance of its users since the coup.

“Two months ago, we [MPT] formed a team to monitor calls. If the system notices a suspicious conversation or detects certain words, the team will be notified. I'm not sure if the recorded



conversations are given to the authorities ... but it's no longer safe to speak on the phone," the official said.

For now, both the police officer and the MPT official recommended people use the foreign-owned operators for safety reasons.

"The regime is likely treating these companies differently because they are foreign and have invested a lot of money – they will be more cautious in how they handle them," the MPT official said.

Mytel did not respond to a request for comment, while a Ministry of Transport and Communications spokesperson said they had no information on the monitoring programme.



MPT office in Yangon. (Frontier)

'They can track what you're looking at'

The authorities have less capacity to monitor internet use than phone calls, the police officer and MPT official said.

"We can only monitor which IP addresses are surfing which websites ... there is no more detail than that because we don't have the technology," the MPT official said.

In mid-March, the regime shut down mobile data entirely, before allowing users to access a [limited internet service](#) of around 1,000 whitelisted websites and applications. "One of the things they are looking for with mobile data surveillance is which sites have slipped through the cracks on whitelisting," the MPT official said.

It's a different picture for fibre internet, the MPT official said. Although most of the internet is accessible – with only some websites and services being blacklisted – the service is fixed to a location and users have to give a significant amount of personal information when they apply for a connection. He said this meant it was important to always use a VPN to ensure your internet activity is not being tracked.

"Unless you're using mobile banking or something like that, you need to use a VPN. If you don't use a VPN, they can track what you're looking at," the MPT source said. "Sometimes the authorities ask us for information about people who are using the [fibre-to-the-home] service. In the past, after we've given this data, I've heard that the person has been arrested."

The cybersecurity team is also monitoring internet use, the police officer said. Its social media monitoring focuses primarily on Facebook, particularly private and public groups, and was responsible for compiling the lists of users facing charges under section 505-A of the Penal Code that were announced in state newspapers each day in March and April.

"I can't say how we monitor Facebook groups – I can only say that people should not discuss anything sensitive in these groups," he said.

The NLD's uncomfortable legacy

Although the systematic monitoring of calls and internet was initiated by the Ministry of Transport and Communications when it was formally under NLD control, the ministry was and continues to be



staffed by many former Tatmadaw officers. “It’s hard to say whether this push came from the Tatmadaw or the civilian side of the government,” the MPT official said.

Among the ministry’s initiatives under the NLD government was a draft Cybersecurity Law, which the military regime inherited and published in early February, in one of its first legislative acts since seizing power. Following [significant pushback](#) from rights groups and business associations, the junta dropped the law but transferred some of its sections to the [amended](#) Electronic Transactions Law of February 15.

The ministry under the NLD also initiated a “lawful interception” programme that would give it direct access to user data from mobile operators and ISPs. Budget documents published by the Open Technology Fund show that the ministry [received](#) the equivalent of US\$4 million to buy equipment for the project in the 2019-20 fiscal year. In December 2020, Telenor [raised the alarm](#) about the programme, warning at a briefing in Yangon that without sufficient safeguards it would create “an opportunity for misuse and breach of customers’ human rights”.

NLD lawmakers also approved budget requests from both the communications ministry and the military-controlled Ministry of Home Affairs for a [range of digital tools](#) – many purchased from companies in Western countries – that in the wake of the coup are being used against regime opponents.

In a recent report, “[Myanmar’s Military Struggles to Control the Virtual Battlefield](#)”, Brussels-based think-tank International Crisis Group said that despite the obvious risks of putting these tools in the hands of the security forces without adequate safeguards, those who tried to raise concerns with the NLD government or party lawmakers were largely ignored.

To rectify the NLD’s missteps, ICG recommended that the parallel National Unity Government, formed in April by ousted NLD lawmakers and ethnic leaders, announce policies that enshrine privacy and affirm its commitment to a free and open internet. The NUG could also use its platform to raise awareness about digital security, for example the importance of using VPNs, the report said.

But the NUG’s Minister for Human Rights U Aung Myo Min told *Frontier* that focusing on military surveillance of phone and internet use risked distracting from the broader goal of revolution.

“Instead of talking about each issue, our goal is just to overthrow the military dictators. Then all issues or problems will be resolved. We want to urge the people to fight this common enemy so that rule of law can be restored,” he said.

On June 5, U Htin Lin Aung was appointed as minister for communications, information and technology in the NUG, but his office did not respond to *Frontier’s* interview request by press time.

More stories



Torture rife in Myanmar’s prisons

Political prisoners released from Myanmar’s jails speak of widespread use of torture by security forces, including death threats, sexual assault and psychological torture.

