



PRESS RELEASE

Myanmar Customers Sue Telecoms Giant Telenor for Sharing Private Data of Dissidents with Military Rulers



DATE

April 08, 2026

CONTACT

Communications

media@opensocietyfoundations.org

OSLO—Today, Swedish non-profit, Justice and Accountability Initiative (JAI) filed a civil class action suit against Telenor ASA before Asker and Bærum District Court in Norway, claiming damages on behalf of Myanmar customers whose data was shared with the military. The case is filed by the Norwegian law firm Simonsen Vogt Wiig and supported by the Centre for Research on Multinational Corporations (SOMO) as well as the Open Society Justice Initiative (OSJI).

Sharing Sensitive Data with the Myanmar Military

Telenor ASA is one of the world's leading telecommunications companies, headquartered in Norway. The Norwegian state is the majority owner of Telenor, holding 54 percent of the shares. With several subsidiaries across the world, Telenor is a key player in the mobile phone service market in Europe and Asia.

Telenor Myanmar Ltd, Telenor ASA's wholly owned subsidiary, commenced operations in Myanmar in 2014 and served more than 18 million customers by 2021. Information Telenor gathered and stored about its customers included name, physical address, Facebook and bank accounts, e-wallets, ID-numbers, location data, and call logs.

On February 1, 2021, the Myanmar military toppled the country's democratically elected government. In the aftermath of the coup, a civil resistance movement was born. The military immediately started cracking down on these activists through widespread arbitrary arrests and detentions, extrajudicial killings, torture, and other forms of serious human rights violations. A civil war between the military junta and forces supporting the opposition continues to date.

In July 2021, despite warnings by civil society organizations and legal action against this transfer, Telenor ASA sold its Myanmar subsidiary. With this transaction, all customer data and active surveillance technology that Telenor had installed were turned over to a military-linked company. Telenor ASA exited Myanmar in March 2022.

Between the time the coup took place and Telenor's exit from Myanmar, the military regularly requested Telenor Myanmar Ltd to disclose specific user data, in particular the data of customers who were suspected of opposing the coup, which the subsidiary handed over. Despite knowing about the risk of human rights violations that were systematically inflicted by the military, Telenor ASA did not prevent the sharing of sensitive data in any of these cases. For some of them, the parent company explicitly recommended compliance with the requests.

Although it is not known exactly how many of these customers' data was shared with the junta by Telenor Myanmar Ltd., the plaintiffs are aware of at least 1,253 phone numbers belonging to users whose data was shared.

Class Action Claim for Damages

The class action lawsuit filed by JAI argues that Telenor ASA is liable for €9,000 in damages per customer whose data was shared because the company either did not prevent disclosure or knowingly and unlawfully authorized the disclosure of their customer data by its subsidiary Telenor Myanmar Ltd. without taking sufficient measures to prevent its misuse.

Under Norwegian law, such conduct entitles affected users to non-economic damages. These intend to compensate the plaintiffs for the impact on their lives beyond financial losses, such as distress and anxiety.

"For us as civil society representatives, we want to hold Telenor accountable on behalf of other users of Telenor, not only for specific people but also for the wider community that was harmed. This is why we are bringing the case," said Ko Ye, chairperson of Justice and Accountability Initiative.

Individual Claims for Damages

In addition, two individuals represented in the case are claiming damages for financial losses. Both Mr. Zeya Thaw and Mr. Aung Thu experienced severe human rights violations after their data was handed over to the military.

Zeya Thaw—From Data Request to Execution

On October 31, 2021, the Myanmar military requested the logs of a phone number owned by Mr. Zeya Thaw, a prominent rapper and lawmaker. After informing Telenor ASA that the request had been made and was going to be complied with, Telenor Myanmar Ltd. handed over the requested data despite an internal assessment that this disclosure was likely to lead to his arrest and affect his right to safety, security, and freedom of expression.

Shortly thereafter, on November 18, 2021, Zeya Thaw was arrested by the military in Yangon. He was convicted in a closed trial and sentenced to death in January 2022. His widow, Tha Zin, read in the newspaper on July 25, 2022 that he had been executed by hanging. She has taken up the case for her husband.

"I lost my husband. It is not just a wife losing her husband. It is also a loss to the movement. It is also a loss to democracy because my husband was committed to democracy and a youth leader. Losing him means a loss to the country," said Tha Zin, individual plaintiff.

Aung Thu—Re-arrest at the Doorstep of Freedom

On September 5, 2021, Aung Thu, a civil society activist, was arrested and charged with sedition, but his case was withdrawn, and he was set to be released. However, on September 22, 2021, the military requested his user data. After escalating the request to the parent company, Telenor Myanmar Ltd. complied with the request, even though an internal assessment found that complying with the request would infringe on internationally recognized human rights.

As he was set to be released on October 17, 2021, Aung Thu was re-arrested at the prison gate. This time, he was charged under terrorism laws and sentenced to five years in prison following a secretive and arbitrary trial. It is likely that the military relied on the shared phone data to convict him in the second proceedings. He was released in 2025 after serving two-thirds of his sentence.

“My lawyers struggled to get information about my case and know about the evidence against me. It was not a fair trial because I did not see any evidence presented in court, and I did not get information about any evidence. I did not know who the witnesses were in my case. In these political trials, they always convict the defendants,” said Aung Thu, individual plaintiff.

Approval at Headquarters (HQ)

The lawsuit argues that Telenor ASA, at its headquarters in Norway, was privy to the military's requests and the inherent risks. A Telenor ASA document contained a standardized procedure for how requests from authorities should be handled by its subsidiaries. In accordance with this protocol, an internal written assessment was prepared by the risk assessment team in Myanmar. Where the requests infringed on human rights or lacked a legal basis, they had to be escalated to Telenor ASA in Norway. At the parent company, the requests were then reviewed by the HQ risk assessment team.

The protocol document appears to envisage that in some scenarios the request would get escalated beyond the HQ risk assessment team to a dedicated committee at the parent company, and then potentially even further to the CEO. However, it is not presently known to the plaintiffs whether, in practice, any requests were in fact escalated beyond the HQ risk assessment team in Norway.

The filings present evidence that several requests were escalated from the Myanmar team to the HQ risk assessment team in Norway, which recommended that Telenor Myanmar Ltd. should comply with the disclosure request from the military. Even when requests were not escalated to Norway, the parent company was regularly informed by its Myanmar subsidiary about the military's data requests through messages between staff in the two locations. Despite this, Telenor ASA appears not to have ever intervened to prevent this practice, thus apparently signaling tacit approval.

“Telenor ASA in Norway clearly contributed to the practice of handing over user data, despite the inherent risks for its customers in Myanmar. We have evidence of cases where the team at HQ expressly recommended the data to be handed over. Even where we do not have this information, we know that staff at HQ would receive regular updates on data requests from a dedicated employee in Myanmar,” said Jan Magne Langseth, lawyer at Simonsen Vogt Wiig.

What's Next

Following the filing of the case, Telenor ASA will have the opportunity to formally respond to the claims. Whilst Telenor's formal response to the claim will be awaited, Telenor's response to the pre-action notice letter on October 20, 2025 was to deny responsibility. In their response, they stated that they were legally required to comply with the requests from the military and had no choice but to comply in order to protect their employees.

Once the court has confirmed whether the case can be tried as a class action, it will schedule a hearing where both parties can present their evidence and oral arguments.

“If successful, this case would be the first ever to hold a telecoms company to account for not sufficiently protecting user data from access by an authoritarian regime. The importance of such a precedent for other companies operating in high-risk countries cannot be overstated,” said Beini Ye, legal counsel at OSJI.

“With authoritarianism on the rise around the globe, this case should serve as a warning not only about corporate control over our data in general but to Telenor specifically, which continues to operate in countries with a heightened risk of data misuse. Stronger privacy laws that give individuals control, stricter limits on data retention, meaningful transparency obligations, responsible exit plans, and enforceable protections that prevent companies from gathering sensitive data in the first place are all examples of what we need,” said Joseph Wilde-Ramsing, director of advocacy at SOMO.

RELATED CASES

LITIGATION**Justice and Accountability Initiative v. Telenor ASA**

The Open Society Justice Initiative is advising plaintiffs and partners in a lawsuit to hold telecommunications giant Telenor to account for sharing customer data with the Myanmar military in the wake of the 2021 coup, leading to widespread human rights abuses.

ALL CASES**TOPICS****Economic Power****Democratic Practice****International Justice****Get In Touch****CONTACT US****Subscribe for Updates About Our Work**

Your email address

By entering your email address and clicking "Submit," you agree to receive updates from the Open Society Justice Initiative about our work. To learn more about how we use and protect your personal data, please view our privacy policy.

What we do

How we work

Who we are

Litigation

Publications

Voices

Newsroom

Contact

© 2026 Open Society Foundations, some rights reserved.

[Terms](#) [Privacy](#) [Cookie Policy](#)