BIZCOMMUNITY

Nigerian military targeted journalists' phones, computers with "forensic search" for sources

By Jonathan Rozen

30 Oct 2019

Hamza Idris, an editor with the Nigerian Daily Trust, was at the newspaper's central office on January 6 when the military arrived looking for him. Soldiers with AK47s walked between the newsroom desks repeating his name, he told CPJ. It was the second raid on the paper that day; the first hit the bureau based in the northeastern city of Maiduguri, where Idris had worked for years.

Hamza Idris (left), an editor with the Daily Trust newspaper, sits with colleague Hussaini Garba Mohammed in their office in the Nigerian capital, Abuja, in February 2019. The office was raided in January by the military, who seized 24 computers. Credit: CPJ/Jonathan Rozen.

The soldiers did not know what Idris looked like and his colleagues did not point him out, he said. Unable to find their target, they ordered everyone to evacuate and seized 24 of the paper's computers. Idris simply filed out with everyone else. In Maiduguri, however, the military arrested Uthman Abubakar, the *Daily Trust* northeastern regional editor, with his two phones and computer, CPJ reported at the time. He was held for two days, interrogated about his sources for a report written with Idris about a military operation in the region, and then released without charge.

"They took the devices to their computer forensics room," Abubakar told CPJ. "They conducted some forensic search."

The *Daily Trust* raids are emblematic of a global trend of law enforcement seizing journalists' mobile phones and computers —some of their most important tools. CPJ has documented device seizures around the world, from the United States to Slovakia to Iraq. In Benin, police copied data from the seized computer of Casimir Kpedjo, the editor of *Nouvelle Economie* newspaper, CPJ reported in April. And in Tanzania, during the detention of two CPJ staff in November 2018, intelligence officers took their devices and boasted about Israeli technology that could extract their information.

Forensics technology designed to extract information from phones and computers is marketed and sold to law enforcement agencies around the world. CPJ has found at least two companies that produce digital forensics tools—Israel-based Cellebrite and U.S.-based AccessData—operating in Nigeria, where CPJ research shows that security forces regularly arrest and interrogate journalists.

Recent Nigerian national budgets feature significant financial allocations to bolster surveillance and digital forensics capacities. From 2014 to 2017, the Nigerian government spent at least 127 billion naira (over US$350 million) on "surveillance/security equipment," according to a 2018 calculation reported by Paradigm Initiative, a Nigeria-based digital

rights group. “Evidence showed that these purchases were made for political reasons, especially by the then authorities in power to monitor their adversaries and political opponents,” that report said.

One of Nigeria’s major security concerns is the years-long conflict in the northeast against Boko Haram and splinter group Islamic State in West Africa Province (ISWAP). Hours before the raids on *Daily Trust*’s offices, the paper had published a report about a Nigerian military effort to retake six towns from Boko Haram. In a statement published on Facebook the next day, a Nigerian army spokesperson said the report had divulged classified information, “undermining national security” and contravening Nigeria’s Official Secrets Act.

Privacy is enshrined in Nigeria’s constitution, and law enforcement agents must obtain a judicial warrant to search computer systems under Nigeria’s 2015 cybercrime law. However, the 1962 Official Secrets Act gives sweeping powers for security forces to grant themselves warrants to search and seize all materials considered evidence, as well as arrest those suspected of committing offenses under the act.

On January 10, four days after the raids, Nigerian military investigators summoned Idris and Nurudeen Abdallah, the *Daily Trust* investigations editor, to question them about their sources for the report, which they refused to reveal, they told CPJ. Then the officers demanded their phones. “They said they want to scan it,” Idris told CPJ. “They said [they] just want to see the contents and then maybe the numbers of the people I talk to—I said no.” The officers told them a server for scanning technology was housed at the Office of the National Security Adviser, the president’s top security aide, Abdallah told CPJ. The journalists said they had not brought their phones, and refused several follow-up requests to return with them.

CPJ reached Sagir Musa, a Nigerian military spokesperson, by phone on October 9 and asked about the *Daily Trust* raids. Musa said he could not hear and asked to be sent a message before the line went silent; subsequent calls and messages went unanswered. Calls to Onyema Nwachukwu**,** director of defense information for the Nigerian military, also went unanswered.

An individual within Nigerian law enforcement told CPJ that security forces use Universal Forensic Extraction Device (UFED) and Forensic Toolkit (FTK) to retrieve information from devices. UFED is sold by the Israel-based company Cellebrite, which is owned by the Japan-based SUNCORPORATION, while FTK is sold by the U.S.-based AccessData Group. The individual agreed to speak to CPJ due to concerns about the technology’s possible misuse, but asked that their name be withheld for fear of reprisal.

Cellebrite’s website says their UFED product can “[e]xtract and decode every ounce of data within digital devices” and that their equipment is deployed “in 150 countries.” Company records stolen by hackers and reported by VICE News in 2017 suggest client relationships with Russia, Turkey, and the United Arab Emirates. U.S. federal law enforcement has also invested in the Cellebrite technology, according to government procurement information listed online and media reports. In Nigeria, “authorities seized [a drug lord’s] Samsung phone” during his arrest “and extracted and analyzed data from it using UFED,” according to a case study publicized on Cellebrite’s website.

Separately, Cellebrite’s UFED was used in Myanmar to “pull documents” from the phones of then jailed Reuters

journalists Wa Lone and Kyaw Soe Oo, *The Washington Post* reported in May 2019. Cellebrite said it required clients to "uphold the standards of international human rights law" or it may terminate their agreements, according to the *Post's* report. Cellebrite's terms and conditions state that products, software, and services are to be used "in a manner that does not violate the rights of any third party."

CPJ reached Christopher Bacey, Cellebrite's director of public relations, by telephone in mid-September to request clarification about the company's sales in Nigeria, and if the company reviews countries' human rights records or considers the rights of journalists to protect their sources. At his request, CPJ sent questions by email, but received no response before publication. Msao Koda, who works in Cellebrite sales for SUNCORPORATION, similarly requested questions by email in September and did not respond before publication.

Like Cellebrite, AccessData advertises FTK as a tool to identify information on "any digital device or system producing, transmitting or storing data," including from web history, emails, instant messages, and social media. It also boasts capacity to "[d]ecrypt files, crack passwords, and build a report all with a single solution."

In 2011, System Trust, a Nigeria-based digital security company, established a sales partnership through DRS, a South Africa-based cybersecurity company, to distribute AccessData technology, the Nigerian *Vanguard* newspaper reported at the time. System Trust CEO Philip Nwachukwu told CPJ by phone that the Nigerian security forces were not among his clients for their technology, but that he was not sure if AccessData had other business relationships in the country. He also emphasized that digital forensics equipment should be deployed ethically. "I can't be a state actor and feel like I have the power, then go and invade the privacy of an individual," he said.

Several CPJ calls to AccessData's corporate headquarters in the U.S. were forwarded by an operator, then rang unanswered. Interview requests sent to two email addresses provided over the phone by people at their London and Frankfurt offices also went unanswered.

CPJ's repeated calls to DRS in early October were forwarded to cybersecurity specialist Zach Venter. On one occasion, Venter asked that CPJ call back after 30 minutes. Subsequent attempts to reach him via phone and messages were unsuccessful.

Uthman Abubakar's devices were returned shortly after his release from detention in Maiduguri, but it was nearly seven weeks before the 24 computers confiscated during the second raid were returned, Mannir Dan-Ali, *Daily Trust*'s editor-in-chief told CPJ. The paper would not be using them again, he said.

For information on digital safety, consult CPJ's Digital Safety Kit.

**Reporting from Abuja, Nigeria and New York.*

ABOUT THE AUTHOR

Jonathan Rozen is a CPJ Senior Africa Researcher.