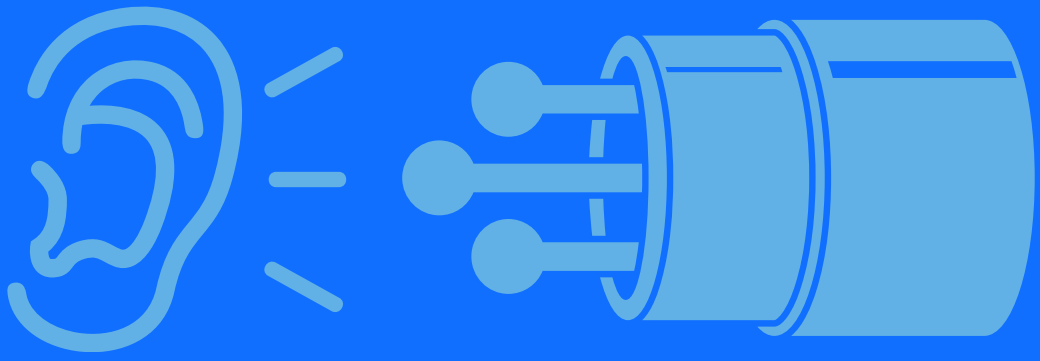
# ADDENDUM: OTHER TECHNOLOGIES TO WATCH

## BULK SURVEILLANCE

Technology exists to monitor and record the landline, mobile, and internet communications of entire countries. Usually, this is done through a device known as an interface that is installed with the cooperation of the telecommunications operator. The interface is connected to the physical network of the operator. It can, for example, tap into fibre optic internet cables, or switching centre equipment. It can then duplicate the digital communication signals passing through the system and reroute it to be recorded for further analysis with computer software.



In South Africa, bulk communications interception is carried out by the State Security Agency's National Communications Centre located in Pretoria. The NCC's purpose is to intercept communications outside of South Africa's borders as part of the countries' foreign intelligence operations. However, communications conducted via the internet usually transverse international borders even if the two people communicating are in the same town. For example, if one sends email via Gmail while you are in South Africa, that message likely passes through Google's servers in the United States. This means that the NCC can in fact intercept domestic communications as soon as those communications leave the borders of the Republic as part of the normal flow of global internet traffic. There is no legislation governing the NCC's operations. In February 2021, the Constitutional Court of South Africa ruled that the NCC's activities were unlawful and invalid.

## THE OFFICE OF INTERCEPTION CENTRES

The Office of Interception Centres (OIC) IS located in Sandton in Gauteng. It is an interception hub for all of South Africa's intelligence services. Its goal is to assist security services to fight crime and terrorism. It is for government use only. This includes the police, the State Security Agency, and military intelligence. As the name suggests, there are satellite interception centres throughout the country, although the exact number could not be sourced for this study. The OIC is capable of monitoring an individual's cellular, landline, and internet communications. This includes landline calls, faxes, cellular calls, SMS messages, emails, social media activity, and data message services (like WhatsApp). The OIC can also monitor metadata (also known as communications-related information). This includes data such as the time and duration of a call and the numbers that were dialled. It also includes location data about the caller's phone.

The OIC is able to intercept communications because of a device known as a handover interface. This is a device installed by the telecoms operator or service provider at their premises. The device can make a digital copy of a surveillance target's communications. This digital copy is then sent to the OIC via a secure cable. The Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002 (RICA) compels all major network operators to purchase, install and operate a handover interface at their own costs. The OIC's primary function is targeted interception.

The OIC can only legally intercept communications through a directive issued by a designated Rica judge. The intelligence services must convince the judge that interception is being used as a last resort, and there must be an existing case docket. Over the past decade, there have been repeated reports of the OIC being misused to spy illegally on journalists and other innocent people. In February 2021, South Africa's Constitutional Court ruled several aspects of Rica to be unconstitutional because it did not safeguard privacy rights sufficiently. Parts of Rica now need to be rewritten.