South Africa's surveillance law is changing but citizens' privacy is still at risk

October 9 2023, by Jane Duncan

Credit: CC0 Public Domain

In a ringing judgment for the right to privacy, the South African Constitutional Court declared sections of the country's main communication surveillance law unconstitutional in February 2021.

The court gave parliament three years to pass a new law remedying the areas of unconstitutionality. The February 2024 deadline for these

amendments is looming fast.

The Regulation of Interception of Communication and Provision of Communication Related Information Act (Rica) was intended in part to protect privacy, combat crime and promote national security. It requires all cellphone sim cards in the country to be registered, and prohibits interception of people's communications without their consent, except under certain conditions.

But Rica had some weaknesses which have been abused by rogue elements in intelligence. The court case was brought by the amaBhungane Centre for Investigative Journalism, after the state misused Rica to spy on the center's managing partner, Sam Sole, in an attempt to reveal his sources of information.

The justice ministry has produced an amendment bill to meet the court's deadline.

Having researched issues relating to communication surveillance and its oversight for years, my view is that the amendment bill is flawed. It doesn't provide enough safeguards against the violation of privacy.

The problem with Rica

In terms of Rica, intelligence and law enforcement agencies must apply to a special, retired judge for interception directions (or warrants) to conduct surveillance to solve serious crimes and protect national security. The judge is appointed by the justice minister.

The court found Rica to be unconstitutional on the following five grounds:

- People don't have to be told that they have been under

surveillance.

- The appointment and renewal processes for the Rica judge lack independence.
- The judge only has to hear from one side: those applying for interception warrants.
- Rica does not ensure that intercepted data is safely managed.
- Rica fails to recognize that lawyers and journalists have a professional duty to keep their sources and communications confidential.

The court prescribed two interim measures while the law was being redrafted. The first was that within 90 days of an interception direction (warrant) having lapsed, those state agencies applying for surveillance need to inform the surveillance subject that they have been spied on. The second is that applicants must also tell the judge if the surveillance subject is a lawyer or journalist.

Post-surveillance notification

With the proposed amendments, the justice ministry has responded largely by reproducing the court's first interim measure. However, it has added another clause stating that if notifying someone that they have been surveilled could potentially have a negative impact on national security, then the judge may withhold notification and for such period as may be determined by the judge.

This clause is too broad and does not provide an ultimate deadline for notification. It introduces speculation into the decision-making. That's because the impact needs merely to be possible. There is no requirement to show a national security threat, merely a possible negative impact.

Independence of the Rica judge

The justice ministry has inserted a requirement for the Rica judge to be appointed by the justice minister, in consultation with the Chief Justice. This is adequate to the extent that it means that decision does not rest with the executive only.

The ministry has also introduced an entirely new position of a review judge, to automatically review the decisions of the Rica judge. It would have been better to build automatic review into the process once surveillance subjects have been notified. That might make the review process more robust as the subject may provide details that shed new light on the Rica judge's decisions. If the judge's decision to grant the warrant was misplaced, this could lead to the original decision being overturned or intercepted material being destroyed.

However, given the load of several hundred cases a year, one judge may not be enough, either at the decision stage or the review stage. Consideration should be given to establishing a panel of judges.

Hearing both sides

It is possible that the review judge was introduced to respond to the problem of hearing only from the applicant (the "ex parte" problem). If that is the case, then it is not an adequate response. Both judges will still be making decisions based on the same one-sided secret evidence.

Rather, as amaBhungane argued in the Constitutional Court case, the bill could include a new position of a public advocate, to defend the interests of the surveillance subjects.

The public advocate could be granted security clearance, in line with well-recognized processes involving "cleared counsel".

Such lawyers have clearance to access the secret evidence the state is

relying on. They are on the same footing as the agency applying for surveillance. They will be able to interrogate the case beyond what is provided for in the application.

As has been argued recently, the public advocate could represent the interests of surveillance subjects who decide to take decisions on review following post-surveillance notification.

Confidentiality for lawyers and journalists

Regarding the need for the applicant to inform the judge that a subject is a journalist or lawyer, the ministry has left out an important safeguard from the interim measure provided by Constitutional Court's judgment. It required the judge to grant the warrant only if necessary, which means that the warrant must be an investigative method of last resort.

On the management of surveillance data, the court required more details in the law on how and where surveillance data must be accessed, stored and destroyed. The justice ministry has failed to provide such detail.

Metadata surveillance

The amendment bill is silent on possibly the most serious surveillance issue, relating to the state's massive and underregulated surveillance of data about a person's communication, or metadata. Rica allows the state to use procedures other than those provided for in the act to access metadata.

For example, the state has preferred to use section 205 of the Criminal Procedure Act as it contains much lower privacy standards than Rica. It is thus open to abuse.

One solution is to make Rica the only law governing access to metadata, but retain the procedure whereby the ordinary courts can grant warrants, rather than restricting decision-making to the Rica judge only, to ensure speedy decision-making.

Missed opportunity

The justice ministry had more than enough time for the review of Rica, section 205 and the entire surveillance setup to assess whether they were still fit for purpose.

The failure is an indictment on the ministry's leadership of the review process. It missed the opportunity to address the growing concerns about unaccountable state spying.

Provided by The Conversation

Citation: South Africa's surveillance law is changing but citizens' privacy is still at risk (2023, October 9) retrieved 27 April 2024 from https://techxplore.com/news/2023-10-south-africa-surveillance-law-citizens.html