To the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

15 February 2019

MISA Zimbabwe's Submission on the Surveillance Industry and Human Rights in Zimbabwe

Zimbabwe has a history of targeted surveillance. Under former President Robert Mugabe's government, the Central Intelligence Organisation implemented low-tech surveillance methods such as physically keeping watch of individuals and listening on their phone calls. In 2015, there were reports that the Iranian government had bestowed surveillance technology upon their Zimbabwean counterparts that included IMSI catchers/ cell tower simulators. Some research has been carried out to detail the use of such equipment in Zimbabwe.[1]

Shortly before his forced resignation, Mugabe set up a Ministry of Cybersecurity, Threat Detection and Mitigation. According to the Presidential spokesperson at the time, the ministry was established to catch "mischievous rats" that abused social media. This would entail that this ministry would carry out some sort of surveillance activities as a means to determine who was abusing social media and who was not.

This ministry was short-lived, as Mugabe's was forced to step down a few weeks later. Under the subsequent government reshuffle, this ministry morphed into a department under the existing Ministry of Information Communication Technologies. It is safe to assume that this Cyber security department will still pursue some of the objectives that it sought to establish during its temporary setting up as a standalone ministry.[2]

The current Zimbabwean government has stepped up efforts to use surveillance technology in the country. In its first official State visit to China in March 2018, a delegation of Zimbabwean government representatives engaged China on a number of partnerships, including the acquisition of Artificial Intelligence based facial recognition software that would be used to maintain "law and order" in Zimbabwe. China's biggest AI firm, *Cloudwalk Enterprises*, will supply this facial recognition technology to Zimbabwe.[3]

There is no evidence yet that the Zimbabwean government has started using this technology in the country. This delay may result from the fact that *Cloudwalk's* AI algorithms still need to be taught how to read and differentiate African faces. To achieve this, the Zimbabwean government reportedly turned over huge amounts of biometric data to the Chinese firm.

Other surveillance-based initiatives include the Smart Cities initiative launched in March 2018.[4] This initiative will see the Zimbabwean government partner with Chinese companies such as *Huawei* for the creation of smart, connected cities. However, this initiative's emphasis has been less about the ways in which IT tools can improve service delivery but it has been more about the installation and use of traffic surveillance cameras and surveillance cameras in public spaces.

[1] https://www.academia.edu/30051415/Use_of_IMSI_Catchers_in_Zimbabwes_Domestic_Law_Enforcement
[2] https://bulawayo24.com/technology/internet/131135
[3] https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/
[4] https://www.ebusinessweekly.co.zw/zimbabwe-the-future-of-smart-cities/

Zimbabwe's two biggest cities have completed pilot projects on the use of surveillance cameras and both cities are set to roll out the technology in the near future.

The challenge with Zimbabwe is that all these developments are taking place in the absence of an adequate data protection and privacy legal framework. This lack of a proper framework leaves citizens' exposed to over surveillance by government and state security forces. The Zimbabwean Constitution does guarantee the right to Privacy but the current law that protects personal information, the Access to Information and Protection of Privacy Act [*Chapter 10:27*] (AIPPA) is woefully outdated and actually narrowly defines the right to privacy.

This week, government publicly declared that it will repeal AIPPA[5] and will replace it with laws that will promote data protection and access to information. However, government did not commit to any timelines on when this would actually happen.

Another challenge is the lack of information and transparency on matters of State sponsored surveillance. The National Assembly is yet to debate issues of surveillance and the various partnership agreements that Zimbabwe enters into to acquire cybersecurity equipment from Asian countries such as China and Japan. Questions around surveillance initiatives in Zimbabwe are dismissed by declaring that those are issues of national security.

AIPPA is supposed to facilitate access to information that is in government's hands, but AIPPA contains blanket exclusions for information that the government may deem to be of relevance to national security.[6] This means that information on the type of surveillance tools used, the frequency of such tools' use and the number of people under surveillance is not available to people outside of the bodies carrying out the surveillance and processing the collected information or data.

Furthermore, the local snooping law, the Interception of Communications Act [*Chapter 11:20*] does not provide for any judicial involvement in the initial issuance of a warrant for interception of communications. Courts are only involved when a government entity wishes to extend the initial six-month surveillance warrant by an extra three months.

The above-mentioned factors all contribute to a situation where the current government is carrying out clandestine surveillance activities. There are no legal frameworks that can be used to compel government to use its surveillance initiatives and at this point, interested organisations and citizens have to rely on media reports to keep informed on government's surveillance initiatives. There is no information on the companies that supply this technology to the Zimbabwean government and how much the government has paid for this technology. Lastly, there is no information about the conditions under which the collected data is processed.

//END

[5] https://www.herald.co.zw/cabinet-approves-aippa-repeal/
[6] Part III and First Schedule of AIPPA