TECHNOLOGY AND COUNTER-TERRORISM:
Mapping the impact of biometric surveillance and social media platforms on civic space

CASE STUDY
UGANDA

This case study was researched and written by Defenders Protection Initiative (DPI), with ECNL's contribution being only editorial input and summarising for the purposes of the report. DPI aims at contributing to the promotion and protection of human rights, good governance, rule of law, peace and democracy by strengthening the capacity of human rights defenders (HRDs) to mainstream security, safety and protection management in their work.

Notable uses of biometric technology

Our research found that existing technologies used for biometric surveillance include digital signal tools, telecom metering systems, drones, CCTV cameras, signal intelligence monitors, and DNA and item scanners,[1] among others.[2] These are deployed in public and private places for policing and security purposes. Additional proposed uses for biometrics include digital drivers licenses, passports, national identification cards, motor vehicle insurance and bugging.[3]

While some digital surveillance tools are deployed in conspicuous places such as airports, highways, school libraries, country border points, and people's home, others are not visible to non-operators.[4] The key justification for such deployment is to ideally have foreknowledge that is required by the state in response to external threats towards life and the wellbeing of its citizens.[5] However, similar operations can also use the collected data for future blackmailing purposes, for example when a political dissident expresses interest in running for political office.[6]

The Ugandan Police Force used facial recognition technology to track anti-government protesters in November 2020.

1 The Uganda Police Force, (2021, January 28). 'Police's Modern Lab Commissioned,' https://www.upf.go.ug/polices-modern-lab-commissioned/

2 Biryabarema, E. (2019, August 15). 'Uganda's cash-strapped cops spend $126 million on CCTV from Huawei,' https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF

3 Akankwatsa, L. (2021, July 14). 'Compulsory GPS tracking of vehicles unconstitutional,' https://observer.ug/news/headlines/70508-compulsory-gps-tracking-of-vehicles-unconstitutional

4 Id.

5 Anonymous. (2021, August 27). The Independent, 'IT experts, security analysts raise red flag on vehicle tracking plan,' https://www.independent.co.ug/it-experts-security-analysts-raise-red-flag-on-vehicle-tracking-plan/

6 Pat, M. (2022, March 1). Kampla Post, 'MPs Demand to Meet Russian Firm over Motor Vehicle Tracking Project', t https://kampalapost.com/content/mps-demand-meet-russian-firm-over-motor-vehicle-tracking-project

Notable uses of online content moderation and social media surveillance

The Ugandan government has sought to censor social media content of CSOs in Uganda, which is viewed by local civil society as a means to restrict their activities online.[7] Criticising the government or calling out police brutality online is often framed as "threats to the security of person or the state."[8] Often, information that supports or promotes the interests and views of the opposition is targeted. The drivers behind such censorship are mainly those affected by the communicated content, namely those with state power and authority. For example, the novelist Kakwenza Rukirabashaija was arrested for his repeated social media posts in which he allegedly harassed President Museveni and the First Son, also the Commander of the Land Forces, Lt Gen Muhoozi Kainerugaba.[9]

The Ugandan Telecommunication Commission's approach towards controlling security threats through social media coverage starts with persuasion, and where that fails, the use of force is deployed.[10] It is imperative to note that there is a relationship between surveillance and action. The interface between the two may result in actions of force. This is where we have witnessed actions of arbitrary arrest, kidnapping, abduction, detention without trial, and sometimes torture of opposition politicians who are first placed under surveillance before arrest.[11]

Some actors[12] suspected of participating in terrorism financing have been banned or profiled, in some instances, their bank accounts have been frozen. A commonly cited example is the National NGO Forum, a network with over 650 member organisations, and the Uganda Women's Network (UWONET), which brings together 20 women's rights organisations and nine individual activists.[13] Their bank accounts were frozen for allegedly committing money laundering and funding subversive activities, including terrorism financing.[14]

7 See for example the Computer Misuse Act-2015 of Uganda; https://twitter.com/jerrybambi1Jerry-Fisayo, B., AF. & Surfshark. (2021). Africanews, 'Uganda, the 15th country in Africa to restrict social media due to elections- report,' 2021. https://www.africanews.com/2021/01/14/uganda-the-15th-country-in-africa-to-restrict-social-media-due-to-elections-report//

8 Id.

9 Kazibwe, k. (2022, January 3). AllAfrica. Uganda: Novelist Kakwenza Arrested for Abusing Museveni, First Son, Says Police https://allafrica.com/stories/202201040131.html

10 Anonymous. (2019, February 6).The independent, 'UCC orders Daily Monitor to shut website,' February 6, 2019 Accessible https://www.independent.co.ug/ucc-orders-daily-monitor-to-shut-their-website/; Anonymous. (2020, February 26. Updated 2020, July 19). The DAILY MONITOR, 'UCC shuts down 30 outdoor community radios,' https://www.monitor.co.ug/uganda/news/national/ucc-shuts-down-30-outdoor-community-radios-1877288

11 Anonymous. (2021, March 11). Human Rights Watch, 'Uganda: End Enforced Disappearances of Opponents,' March 11, 2021. Accessible at https://www.hrw.org/news/2021/03/11/uganda-end-enforced-disappearances-opponents

12 Information as part of this case study comes from personal interviews. Names have not been included due to fears over security.

13 Draku, F. (2020, December 2). The DAILY MONITOR, 'Govt freezes accounts of 4 NGOs doing poll work,' https://www.monitor.co.ug/uganda/special-reports/elections/govt-freezes-accounts-of-4-ngos-doing-poll-work-3216360

14 Anonymous. (2020, December 13). The Independent, 'CSOs condemn gov't for freezing NGO accounts,' https://www.independent.co.ug/csos-condemn-govt-for-freezing-ngo-accounts/

The Ugandan Human Rights Commission has institutional mechanisms for addressing grievances of groups and human rights organisations who experience abuse. However, in addition to fears of security and safety, several civil society activists and human rights defenders were unwilling to comment regarding the reliability of their information and data protection vis-à-vis the possibility of hacking their "private" content.

Relevant laws and legal precedents

The Data Protection and Privacy Act (2019)[15] sets out major compliance principles for data protection by key players along the data value chain (data collectors, data processors, data controllers). However, there's also a high risk that unethical powerful actors weaponize the law to silence dissenting voices. Authorities had already previously manipulated data under their control to the detriment of the data subjects.

According to an undisclosed source, Uganda's government has been considering incorporating human rights impact assessments in its new law on privacy rights and data protection.

Data-sharing between private companies and the state

The government of Uganda collaborates with the private sector for strategic value intelligence gathering. Through this collaboration, the government has collected and mined data via high-tech surveillance tools extended to the Uganda government by Russia and China. A noteworthy example is collaboration with the Russian company Joint Stock Company Global Security.[16]

The Ugandan government also partners with telecommunication companies, such as Airtel and MTN, to develop an app to track and trace criminals, including terrorist suspects. Deployment is yet to be made operational and there are no clear timelines. Most importantly, such partnership and the resulting app have severe risks for civic space and human rights, given how the app can be misused and abuse to target CSOs.

15 Data Protection and Privacy Act, 2019 Act 9 of 2019 (2019, May 3). https://media.ulii.org/files/legislation/akn-ug-act-2019-9-eng-2019-05-03.pdf

16 URN. (2021, July 25). The Observer, 'Company awarded 10-year digital tracking contract facing bankruptcy in Russia,' https://observer.ug/news/headlines/70640-company-awarded-10-year-digital-tracking-contract-facing-bankruptcy-in-russia

Unique aspects of the local surveillance landscape

Beyond social media and biometric surveillance, governments have for years resorted to forms of surveillance, including human surveillance, image surveillance, signal surveillance, measurement and signature surveillance.[17] All use violates the right to privacy when deployed arbitrarily without judicial oversight, prescribing the perimeters within which it must be undertaken. Urgent and meaningful participation of civil society is required in the country's legal framework. This is especially important as the general public has limited knowledge about the effects (including spillover effects) and risks related to surveillance.

17 Protection International, 'Surveillance And Counter-Surveillance For Human Rights Defenders And Their Organization', 2014.

European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt
2513 AM, The Hague
Netherlands

www.ecnl.org
@enablingNGOlaw