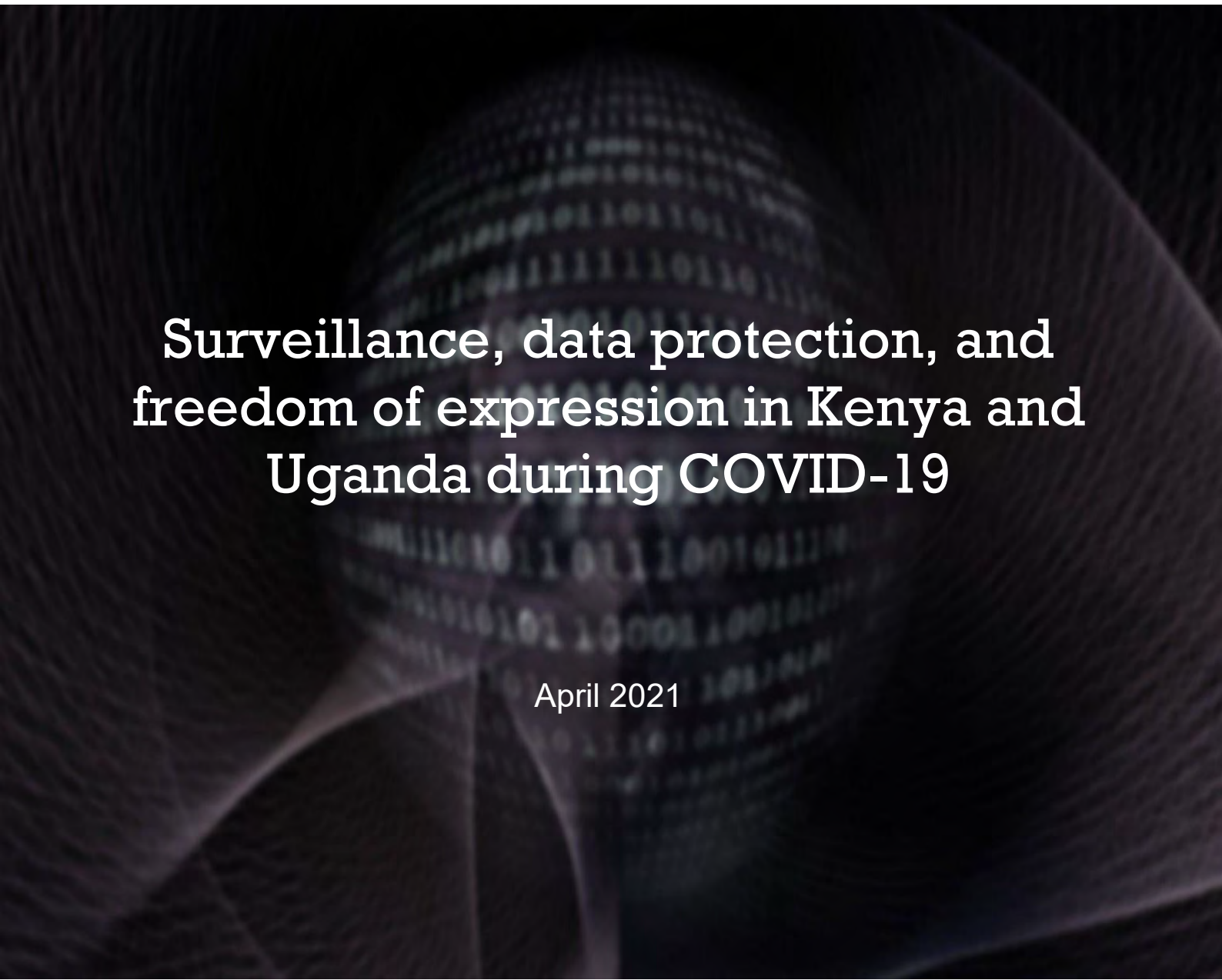
# Unseen Eyes, Unheard Stories



## Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19

April 2021

**ARTICLE 19 Eastern Africa**
Nairobi, Kenya.

**E:** kenya@article19.org
**W:** www.article19.org

**Kenya ICT Action Network**
Nairobi, Kenya.

**E:** info@kictanet.or.ke
**W:** www.kictanet.or.ke

**Pollicy**
Kampala, Uganda.

**E:** info@pollicy.org
**W:** www.pollicy.org

Created in partnership with ARTICLE 19 Eastern Africa, the Kenya ICT Action Network and Pollicy.

**Lead researchers:** Sigi Waigumo Mwanzia, Victor Kapiyo, and Phillip Ayazika.

A19/EAF/2021/002

ISBN: 978-9966-084-18-7



This publication is wholly financed by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA). CIPESA does not necessarily share the opinions expressed here. ARTICLE 19 Eastern Africa, the Kenya ICT Action Network, and Pollicy bear sole responsibility for the content.

# Contents

# Executive summary

**This report by ARTICLE 19 Eastern Africa, the Kenya ICT Action Network (KICTANet), and Pollicy reviews the national legal frameworks and practices that have enabled an extraordinary surveillance environment during the first year of the coronavirus pandemic in Kenya and Uganda. It documents and raises awareness about government and private sector surveillance measures and practices in both countries during this period and their human rights implications.**

Addressing the coronavirus pandemic has required effective responses by governments, private actors, and the international community generally, including tracking the infection rates and preventing the spread of the coronavirus disease. While digital technologies can assist in the delivery of such responses, surveillance technologies raise significant risks for human rights, including the rights to privacy, data protection, freedom of expression, and access to information.

Tackling the COVID-19 public health crisis in Kenya and Uganda was not matched with a prioritisation of human rights protections. In both countries, **the surveillance environment expanded** against a backdrop of weak accountability and transparency and the non-proactive disclosure of information about both governments' responses to the pandemic.

The following key trends were observed in Kenya and Uganda:

- The surveillance measures and practices adopted to contain the COVID-19 pandemic, including coronavirus applications (apps), did not comply with the three-part test under international law and national laws guaranteeing the rights to privacy, data protection, freedom of expression, and access to information.

- Data protection authorities are not independent, and they lack the functional and operational capacity to oversee surveillance measures and practices to contain the COVID-19 pandemic.

- State actors and private entities have collected, processed, and shared personal data, including sensitive health data, in **breach of data protection principles and safeguards in national data protection laws**. In particular, they failed to integrate data protection principles, including purpose limitation, data minimisation, data retention, and prior and informed consent, into the design, development, and deployment of technologies, products, and services to tackle the COVID-19 pandemic.

- Despite reports of close collaboration between state agencies and private actors to deploy digital technologies as part of pandemic measures, there is **no transparency about these partnerships**. While there have been press reports detailing collaboration on digital contact tracing initiatives, there is **no publicly accessible information** about public–private contracts, data sharing agreements, architecture of the technologies, budgetary allocations, or procurement processes of these pandemic surveillance technologies.

We hope the report will be a useful resource for government policymakers and agencies, the private sector, activists, journalists, and human rights organisations in Kenya and Uganda, in their work towards promoting the rights to privacy, data protection, freedom of expression, and access to information.

# Introduction

**Kenya**[i] and **Uganda**[ii] both confirmed their first cases of COVID-19 on 13 and 21 March 2020, respectively. These announcements resulted in a raft of measures taken at the strategic, policy, regulatory, and legislative levels to control the spread of the pandemic. Measures included the suspension of public gatherings, social distancing requirements, local and international travel restrictions and limitations, imposition of curfews, mandatory quarantine, and new laws to formalise the measures. Under the guise of public health protection, both governments utilised existing surveillance practices such as closed circuit television (CCTV) and communications surveillance (mobile phone monitoring using location data) and augmented them with new COVID-19 surveillance laws and measures, including digital contact tracing.

The recently enacted data protection laws in both countries[iii] were expected to provide a framework for the transparent and rights-respecting collection of personal data. However, the documented surveillance trends and **unsupervised** collection of data during the first year of the pandemic revealed two issues.

First, the lack of independent supervision of these data protection laws resulted in poor enforcement and implementation of obligations which apply to data controllers and processors, including public health authorities. Second, this supervision challenge did not limit or check the surveillance capabilities and practices of state and non-state actors. For example, state actors continued to use CCTV cameras with biometric features for mass surveillance in public or publicly accessible spaces, which compromised individuals' privacy and personal data. Instead, the Ugandan Government announced that it would use the data protection law to prosecute individuals for 'spreading misinformation and fake news'[iv] whereas the Kenyan Government used the Data Protection Act 2019 to charge a blogger, Edgar Obare, with unlawfully disclosing the personal data of a Kenyan YouTuber.[v]

Under international human rights law, governments must protect human rights at all times, while corporate entities have a baseline responsibility to respect human rights in all situations.[vi] As such, the pandemic must not be used as an excuse to normalise data collection and unsupervised intrusion and control over people. Specifically, digital surveillance measures, even during periods of crisis, must conform to the requirements of legality, legitimacy, necessity, and proportionality as provided under international human rights law.

When examining these concerns in detail, the report first sets out the legal standards on surveillance and human rights at the international, regional, and national levels. Building on these standards, the second and third sections review the general risks and challenges associated with COVID-19 surveillance measures and coronavirus applications, respectively. Finally, the report offers recommendations on how to ensure that these surveillance measures comply with international human rights laws, standards, and best practices.

## Methodology

The project partners selected Kenya and Uganda for this review because these are the only East African countries to have enacted data protection laws prior to the COVID-19 pandemic and to have established data protection authorities. The findings from Kenya and Uganda set a regulatory standard for the East Africa region, albeit a weak one, for the collection and processing of personal data and the deployment of existing and new laws, practices, and technologies to address the current and future public health crises of a similar scale.

The report is based on regular monitoring of developments in Kenya and Uganda as reported in print and digital media, information provided directly by data subjects and coronavirus app users, and an assessment of statements issued by state agencies and their representatives. Data protection legislation and pandemic surveillance laws, regulations, rules, policies, and

guidelines from both countries were also reviewed. The examination of coronavirus apps relied on information from Google Play store and reports generated on the privacy audit platform for Android app, Exodus Privacy. In addition, the information in the report builds on previous reports and analyses on privacy, access to information, freedom of expression, and pandemic surveillance published by the three partners in both countries.

The information gathered in this report is based on evidence in the public domain and information obtained by the project partners, including official communication to governments and private sector entities. We note that there were limitations to the study that impacted our ability to cover the topic with more depth and complexity. These include poor reporting and documentation by state and private actors, limited data and reliable information on the topic, and individuals' reluctance to provide first-hand experiences about surveillance measures in Kenya and Uganda.

# Applicable standards on surveillance and human rights

## International and regional frameworks

Mass and targeted surveillance and unsupervised data collection impact human rights, including the rights to privacy, data protection, and freedom of expression and information.

The rights to privacy, freedom of expression, and access to information are mutually reinforcing – all the more so in the digital age.[vii] These rights are enshrined in the Universal Declaration of Human Rights (UDHR) and given legal force by the International Covenant on Civil and Political Rights (ICCPR), and the African Charter on Human and Peoples' Rights (African Charter).[viii] Likewise, these rights are protected in the national constitutions of both Kenya and Uganda.

The **right to privacy** is a powerful bulwark against state and corporate power, and serves as a 'gateway to secure [the] exercise of the freedom of opinion and expression' and the right to access information.[ix] The right to privacy also encompasses the protection of personal data.[x] In the context of digital surveillance, these rights, when properly balanced,[xi] are 'designed to empower the citizen to protect their rights'[xii] and to improve the transparency and accountability of public and private bodies that collect, use, and disseminate personal information in information systems and through 'tools of digital surveillance'.[xiii]

While protections against arbitrary or unlawful surveillance have focused on guaranteeing the right to privacy, these interferences also have a chilling effect on the rights to **freedom of expression and information**, **and assembly and association**. For instance, the deployment of secretive, mass surveillance programmes 'renders it practically impossible for any layperson to discern which forms of communication and data storage are secure and when they may be reasonably subject to surveillance.'[xiv] Studies also reveal that the use of surveillance technologies and people's awareness of being watched and tracked 'might lead to people's refusal to join public assemblies, participating in social and cultural life, and feeling constrained to freely express their thoughts, conscience and religious beliefs in public spaces.'[xv]

The rights to privacy, data protection, freedom of expression and access to information are not absolute. They are subject to permissible limitations applying to the right to freedom of expression under Article 19 of the ICCPR and the right to privacy under Article 17 of the ICCPR.[xvi] Based on this, a state may exceptionally limit the rights to privacy, data protection, freedom of expression, and information, provided that the limitation is:

- Provided for by law – any law or regulation must be formulated with sufficient precision to enable individuals to regulate their conduct accordingly;

- In pursuit of a legitimate aim, listed exhaustively as: respect of the rights or reputations of others, the protection of national security or of public order (ordre public), or the protection of public health or morals; and

- Necessary and proportionate in a democratic society, for example if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.[xvii]

Accordingly, surveillance measures implemented to promote public health and contain the COVID-19 pandemic such as the interception of communications and contact tracing using, for example, location data and coronavirus apps, must be carried out strictly in line with human rights standards.[xviii] The deployment of these surveillance measures risks entrenching a 'surveillance infrastructure' permitting both state and public actors to 'continuously monitor individuals' movements'.[xix] These interferences with the rights to privacy, data protection,

freedom of expression and freedom of association 'could violate rights and degrade trust in public authorities – undermining the effectiveness of any public health response.'[xx] 'Track and trace' measures must also be 'implemented with transparency and adequate oversight. What this means in practice is that surveillance measures must be the least intrusive available to achieve the desired result.'[xxi]

Human rights bodies have already raised concerns about the compliance of a number of COVID-19 pandemic measures, including surveillance measures using digital technologies, with human rights:

- In his July 2020 report to the UN Human Rights Council, the UN Special Rapporteur on the right to privacy (Special Rapporteur on Privacy)[xxii] warned that although international law provides for the temporary increase of special powers during the COVID-19 pandemic, various minimum requirements must first be met. These include legislative safeguards ensuring that 'surveillance cannot be initiated until, or unless, it is proven to an independent and competent authority that such surveillance is legal, necessary and proportionate to the objective pursued.'[xxiii] Significantly, the use of generic legal provisions, including those permitting public health authorities to 'order such other action be taken as he [or she] may consider appropriate', were deemed to offer inadequate safeguards.[xxiv] Moreover, the deployment of a surveillance apparatus must be time bound, and deployed for a specific purpose. Here, the Special Rapporteur decried the deployment and use of surveillance apparatuses originally intended for state security purposes to tackle the pandemic.[xxv]

- Earlier, when commenting on the issue of the use of smartphone and contact tracing apps, the Special Rapporteur on Privacy affirmed that 'sole reliance on legal safeguards is not enough. Privacy should be considered from the very beginning, starting with the engineering of the application.'[xxvi] Here the core considerations that must be taken into account include whether the app uses a centralised or decentralised approach, whether the app is deployed using mandatory or voluntary approaches, whether free consent is prioritised, and whether anonymisation and encryption safeguards exist. Additionally, the Special Rapporteur on Privacy emphasised that any compulsory data entry by individuals in the apps must be assessed against the principles of data minimisation, necessity and retention, purpose limitation, and storage safeguards.[xxvii]

- Likewise, the High Commissioner for Human Rights and the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur on Freedom of Expression) both highlighted cross-cutting challenges contributing to a lack of accountability, enabling unlawful digital surveillance and arbitrary inferences of the right to freedom of expression and privacy. These include 'weak regulatory environments, a lack of adequate national legislation and/or enforcement, weak procedural safeguards and ineffective oversight.'[xxviii]

Communications surveillance put in place to (supposedly) help with the pandemic can deprive people of their **right to remain anonymous**, which is central to the rights to free expression and privacy. Anonymity and encryption measures enable 'private communications and can shield an opinion from outside scrutiny, [which is] particularly important in hostile political, social, religious and legal environments.[xxix] For example, individuals who use encryption and anonymity tools are empowered to 'circumvent barriers and access information and ideas without the intrusion of authorities', especially in environments where filtering and other unlawful censorship methods and technologies are used.[xxx] Various groups, including journalists, human rights defenders, and civil society representatives, rely on these measures and tools to ensure they 'shield themselves (and their sources, clients and partners) from surveillance and harassment'.[xxxi] The High Commissioner for Human Rights, commenting on the impact of new technologies on peaceful protests and the realisation of the right of peaceful assembly, emphasised that encryption and anonymity measures help to protect the confidentiality of digital communications for protesters (organisers and participants) who are being surveilled.[xxxii]

For these reasons, both the High Commissioner for Human Rights and the Special Rapporteur on Freedom of Expression noted that 'encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief'.[xxxiii] The African Declaration on Internet Rights and Freedoms, Principle 8, reiterates that everyone has the 'right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.'[xxxiv] The Necessary and Proportionate Principles maintain that 'States should therefore refrain from compelling the identification of users.'[xxxv]

The Special Rapporteur on Freedom of Expression stressed that encryption is a fundamental feature enabling anonymity, and any restrictions must satisfy the three-part test permitting the limitation of the right to freedom of expression under international law.[xxxvi] Therefore, it is important that states provide guarantees of anonymity (or do not suppress it more than is necessary and proportionate) in laws that enable communication surveillance.[xxxvii]

**Targeted surveillance measures** deployed during the pandemic **and search powers granted to medical officers** to control the COVID-19 pandemic must be subjected to judicial oversight and be carried out in line with human rights standards. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism argued that:

> *"States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack."*[xxxviii]

The Special Rapporteur on Privacy commented that the search and seizure powers of public health authorities are often 'greater than those of the police' but that these are rarely reported on due to a 'presumption in favour of public health'.[xxxix] When addressing ordinary and extraordinary public health situations that can give rise to legitimate situations where the rights to privacy and expression can be limited, the state must still demonstrate either a 'particularised factual basis or adherence to the three-part test'.[xl] The failure to subject the powers of medical officers and inspectors to judicial oversight therefore sets a subjective and potentially limitless standard for interference with the rights to privacy and expression, without indicating how and when these powers can be deployed or delegated.

### Responsibilities of the private sector

While international human rights law places obligations on states to protect, promote, and fulfil human rights, business enterprises also have a responsibility to respect human rights.[xli] Importantly, UN Special Rapporteurs on Freedom of Expression have argued that 'censorship measures should never be delegated to private entities', with calls for an 'immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways.'[xlii]

## National frameworks

Kenya and Uganda both provide **constitutional protections** for the rights to privacy, freedom of expression, and access to information. Kenya's Constitution explicitly provides for the protection of the right to privacy under Article 31, freedom of expression under Article 33, and access to information under Article 34. Uganda's Constitution explicitly provides for the protection of the right to privacy under Article 27, freedom of expression under Article 29, and access to information under Article 41.

Both countries do not explicitly recognise the right to anonymity as part of the rights to privacy and freedom of expression. Instead, several laws restrict the ability of individuals to

protect the confidentiality of their communications. While Kenya has not placed any restrictions on the use of encryption tools, anonymous communication is limited by mandatory SIM card registration requirements in the Kenya Information and Communications (Registration of SIM-Cards) Regulations, 2015.[xliii] In the aftermath of the 2021 Ugandan elections, the government threatened to arrest users of Virtual Private Networks (VPNs) which imposed restrictions on the use of encryption tools in the country.[xliv] The ability of individuals to communicate anonymously is also compromised by mandatory SIM card registration requirements under the Regulation of Interception of Communications Act, 2010; the Regulation of Interception of Communications Instrument, 2011; the Registration of Persons Act and Regulations, 2015; and mandatory prior authorisation and registration requirements for online content providers.[xlv]

Both countries enacted **data protection laws** before the COVID-19 pandemic, giving further effect to the rights to privacy, data protection, freedom of expression, and access to information. Kenya enacted the Data Protection Act, 2019 in November 2019, while Uganda enacted the Data Protection and Privacy Act, 2019 in February 2019.

In addition to these challenges, there are several laws in both countries that limit the rights to privacy, data protection, freedom of expression, and information. Prior to the emergence of the COVID-19 pandemic, both Kenya and Uganda implemented various laws permitting the interception and surveillance of communications and broad search and seizure powers.[xlvi] In Kenya, these laws include the Kenya Information and Communications Act (CAP 411A), the Prevention of Terrorism Act, 2012, the National Intelligence Service Act, 2012, and the Computer Misuse and Cybercrimes Act, 2018. In Uganda, these laws include the Regulation of Interception of Communications Act, 2010 and the Computer Misuse Act, 2011. These laws have been abused and are continuously used by state security agencies to target, intimidate, arrest, and arbitrarily detain government critics, journalists, and bloggers.[xlvii]

During the pandemic, both Kenya and Uganda expanded public health legislation which promoted the adoption and use of surveillance measures, including contact tracing and quarantine surveillance.[xlviii] In Kenya, the government issued the Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020 under the Public Health Act (CAP 242). In June 2020, the Ministry of Health released the *Home Based Isolation and Care Guidelines for Patients with COVID-19*.

Similarly, Uganda's Minister of Health expanded Section 36 of the Public Health Act (CAP 281) and issued the Public Health (Control of COVID-19) Rules, 2020 and the *Guidelines on COVID-19 Self Quarantines*. The Ugandan Government also prepared an enhanced surveillance strategy to promote contact tracing and quarantine surveillance measures, which is valid until June 2021.[xlix]

On a positive note, Kenya's Data Commissioner issued a draft *Guidance Note on Access to Personal Data during COVID-19 Pandemic* which was released to the public for comments (i.e. public consultation) in January 2021. This note offers guidance to 'any person processing personal data of individuals to actualise responses and research on the pandemic'. Significantly, this note acknowledges that health data and geo-location may be necessary for contact tracing, but confirms that these are subject to the Data Protection Act, 2019.

At a substantive level, Kenya's draft guidance note is a step in the right direction because it provides policy guidance to both state and public actors who are accessing and processing personal data for response and research purposes during the pandemic. This document clarifies that the Data Protection Act, 2019 applies to the processing of health and geo-location data during the pandemic. Commendably, the draft guidance note mandates any person sharing personal data to publish policies detailing the information being collected and the persons with whom the information may be shared. Lastly, the guidance note mandates that personal data must be presented in an 'anonymized format and in a manner that individuals cannot be re-identified'.

In May 2020, Uganda's National Information Technology Authority (NITA-U), Uganda's information and communications technology (ICT) regulatory authority, published a privacy policy for the COVID-19 ('Coronavirus') tracing app. This was developed by the Ministry of Health and NITA-U.[i]

# COVID-19 surveillance trends in Kenya and Uganda

In both countries, existing and new surveillance measures were used to 'track and trace' individuals suspected to have or who had contracted the COVID-19 virus. These measures were deployed in environments where compliance with legal and human rights standards was inadequate, which heightened the risk of human rights violations.

In this section, seven trends affecting the rights to privacy, data protection, freedom of expression, and access to information in Kenya and Uganda are explored. These include poor oversight over COVID-19 data collection; lack of independent data protection authorities; disclosure of personal data without consent; the use of telecommunications data to 'track and trace' individuals; surveillance of public spaces using CCTV and biometric technologies; broad search powers to medical and public health officers; and the lack of transparency and accountability by state and non-state actors.

## Poor oversight over COVID-19 data collection

Data protection authorities in both Kenya and Uganda were not constituted at the time the pandemic struck, and as such, they were not present to oversee COVID-19 data collection during the first year of the pandemic. Upon their constitution, they have yet to take and implement concrete steps to provide oversight of data collection during this period.

For example, Kenya's draft *Guidance Note on Access to Personal Data during COVID-19 Pandemic* was only issued ten months after the government's official announcement of the pandemic and the deployment of disease surveillance measures. Further, the note falls short of the standards set out in the UN's *Recommendation on the Protection and Use of Health-related Data*, which provide a 'common international baseline for minimum standards of protection for health data'.[li] This guidance note also fails to mandate the disclosure of data sharing agreements that would greatly promote transparency and accountability and contribute to Kenya's Open Data commitments. The guidance note has not been formally adopted and was conspicuously absent from the six products which were launched by the Office of the Data Protection Commissioner[lii] during the release of the 100-day status report on 24 February 2021.[liii]

Unlike Kenya, Uganda's NITA-U has not published guiding principles for the collection, use, and processing of COVID-19 data generally.

## Lack of independent data protection authorities

Both countries opted to establish **data protection authorities** as state agencies rather than as independent or autonomous bodies.

Kenya's data protection authority is established as a state agency under the Ministry of ICT as per Section 5 of the Data Protection Act, 2019.[liv] In Uganda, the data protection authority is situated as an office within NITA-U as per Section 2 of the Data Protection and Privacy Act, 2019.[lv] NITA-U is supervised by the Ministry of ICT & National Guidance.[lvi]

Establishing a completely independent and autonomous data protection authority is an international best practice which is linked to the promotion and protection of the constitutional right to privacy. Studies indicate that independence 'incorporates both positive independence – independence to carry out functions in a certain manner – and negative independence – independence from external influence'.[lvii]

From an autonomy perspective, it will be difficult for these authorities to oversee the activities of government bodies superior to them (for example, a Ministry in Kenya or a statutory body in Uganda overseen by a Ministry), irrespective of checks and balances or statutory guarantees of independence. This structure also effectively limits the ability of the data

protection authorities to exercise appropriate oversight over *all* public bodies and organs. This is prejudicial to the right to privacy and will hamper their mandate in ensuring accountability, good governance, integrity, transparency, and oversight of data collection programmes.

At the staffing level, neither of the authorities have sole responsibility and powers to appoint officers and staff to ensure the proper discharge of their functions.[lviii] In Kenya, the data protection authority must consult and rely on two executive bodies – the Public Service Commission and the Salaries and Remuneration Commission – on staffing and remuneration issues. It is unclear whether the data protection office has the final say in these determinations.

In Uganda the situation of the data protection authority as an office within NITA-U could present challenges for the office in delivering its mandate for various reasons. First, given the NITA-U structure, the data protection function is new and may not be prioritised within the organisation. Second, the office will be in competition for financial and human resource allocations with NITA-U's existing programmes. Third, the data protection law does not provide the criteria and mechanism used to appoint the national personal data protection director or the officers, which is left to the discretion of NITA-U's Executive Director and Board.[lix] Uganda's draft Data Protection and Privacy Regulations, 2020 does not comprehensively address these challenges and is not yet operational.

At the budgetary level, Kenya's data protection law provides that funding for the data commissioner's office can be obtained from both public and private sources, including grants, gifts, and donations. Uganda's data protection law is silent on the funding mechanisms for the data protection office, but the NITA-U Act specifies that funding can be obtained from parliament, and revenue collected from services, loans, and grants.[lx] The failure to provide both data protection authorities with an annual budget which is separate and independent from their line ministries and directly approved by parliament *only* gives rise to the presumption that the line ministries could influence or control both authorities through the budgetary process.[lxi] In comparison, the EU General Data Protection Regulation calls on Member States to ensure that any form of financial control over a supervisory authority 'does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget'.

## Disclosure of personal data without consent

In Kenya, Section 60 of the Public Health Act (CAP 242) grants powers to port health officers to require, at any time, any person on any vessel to answer 'any question' for the purpose of ascertaining whether or not infection exists or has recently existed on board. Pursuant to this, the Ministry of Health requires travellers into and out of Kenya to complete the Travelers Health Surveillance Form and provide personal information, including their name, date of birth, gender, nationality, country of origin, phone number, email address, and destination, and answer a list of questions to determine whether they have had any COVID-19 symptoms.

Further, Rule 2 of the Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020 imposes a responsibility on every owner, person in charge of, or occupier of premises, and every employer and head of a household to notify multiple government agencies of any person suspected to be suffering from COVID-19 in their premises. Under the *Home Based Isolation and Care Guidelines for Patients with COVID-19*, persons under isolation and all household contacts are required to complete a symptoms-reporting schedule for up to 14 days. This information feeds into Kenya's Jitenge System, which will be examined later.

In Uganda, the *Guidelines on COVID-19 Self Quarantine* require individuals to provide their name, next of kin, physical address, and telephone contact, and permit government surveillance teams to monitor individuals for 14 days.[lxii] Uganda's Public Health (Control of

COVID-19) Rules, 2020 have a similar responsibility for notification as Kenya's Public Health Regulations.

In both countries, this collection of personal data is subject to the data protection laws. However, the public health laws in Kenya and Uganda fail to justify how this data collection is necessary and proportionate to achieve the protection of public health. Further, these laws fail to clarify where the personal data which has been collected is stored and for how long, and how this data will be used and by whom.

## Use of telecommunications data to 'track and trace' individuals

In Kenya and Uganda, telecommunications data – specifically, location and call data from smartphones – was initially used by governments to track and trace individuals and enforce quarantine surveillance, before coronavirus apps were proposed, developed, or used.[lxiii] Governments relied on national security and public health considerations to justify limiting the right to privacy and data protection, without regard for due process.

Instructively, in Kenya, telecommunications data was used to track, in real-time, the 'mobile phones of people suspected to have COVID-19 as a way of enforcing a 14-day mandatory isolation period' or individuals entering Kenya from points-of-entry, for example airports, who committed to self-quarantine.[lxiv] Additional reports indicate that the National Intelligence Service used phone data to trace patients' movements.[lxv] These individuals were 'not supposed to switch off their gadgets', as a breach of these government conditions could result in individuals being detained in government-run surveillance facilities.[lxvi] In March, a report emerged that a woman travelling from the UK to Kenya who breached the self-quarantine directive by going to her place of work was tracked using her mobile phone and 'taken away to a government medical facility'.[lxvii]

In Uganda, MTN Uganda and NITA-U partnered to develop the E-pass app, which was launched in March 2021.[lxviii] The app relies on geofencing technology to track and trace the movements of COVID-19 patients under the Ministry of Health's home-based care programme.[lxix] When a patient under home-based care leaves their location boundary, the E-pass app alerts the Ministry of Health designated officials and enables them to locate the patient and their contacts.[lxx] It is unclear how many people have been tracked and traced using this app.[lxxi]

At the East African Community (EAC) level, Partner States rolled out the Regional Electronic Cargo and Driver Tracking System (RECDTS), a digital monitoring and surveillance tool.[lxxii] The RECDTS leverages interstate truck drivers' mobile phones to track and trace their movements within the EAC, the Common Market for Eastern and Southern Africa (COMESA), and the Southern African Development Community (SADC) regional blocs.[lxxiii] The RECDTS and the Corridor Trip Monitoring System were developed for, inter alia, the 'recording, monitoring and surveillance of driver and crew wellness including medical test results for specified communicable diseases such as COVID-19, tracking of vehicles, loads and drivers and crew, and contact tracing.'[lxxiv] These surveillance systems are integrated into trade and transport guidelines addressing the COVID-19 pandemic, and span the three regional blocs.[lxxv]

In view of this, the use of telecommunications data for quarantine surveillance and contact tracing purposes 'to aid the monitoring and enforcement of social distancing'[lxxvi] raises core concerns for the rights to privacy and expression. It is imperative to ensure that these practices are deployed with sufficient guarantees for people's rights and not regularised beyond the crisis given the risks of mass surveillance, fears of continuous monitoring of individuals in both public and private spaces, and data misuse.

The Kenyan and Ugandan Governments failed to pass laws that regulate and minimise instances where mobile operators are allowed to 'share with authorities the geo-location data of self-quarantined patients with confirmed COVID-19 to monitor that the patients indeed

observe self-quarantine',[lxxvii] while also providing guarantees during this data sharing. Further, state agencies and private entities in both countries have not disclosed the full extent of the data sharing activities, through the publication of information and data on publicly accessible platforms (open government platforms), and via publicly accessible resources (corporate transparency reports). In addition, the data sharing activities took place in an environment of weakened transparency and the lack of accountability by both state and non-state actors, making it difficult to conclusively determine whether privacy, data protection, and freedom of expression safeguards were applied.

Similarly, while regional efforts at the EAC level were taken to address the pandemic, including data sharing using systems such as the RECDTS, the cross-jurisdictional implications of such data collection systems remain unknown. Despite a Data Privacy Policy guiding the deployment of the RECDTS and the collection and sharing of personal data by multiple states, this document has not yet been signed by Partner States in the three regional blocs and appears to have no legal force in both Kenya and Uganda.[lxxviii] At the EAC level, heads of states continue to withhold their assent to the EAC Human and Peoples' Rights Bill, 2011), which contains an explicit (sub-regional) right to privacy under Article 19 of this bill.[lxxix]

## Surveillance of public spaces using CCTV and biometric technologies

During the first year of the pandemic, the Kenyan and Ugandan Governments relied on CCTV surveillance to monitor public spaces and enforce social distancing requirements.

The Kenyan Government deployed, in public spaces, a fully-operational mass surveillance system, including CCTV cameras, with facial and movement recognition capacities in real-time.[lxxx] In April 2019, the President of Kenya confirmed that 'almost 2,000 CCTV cameras are working in Nairobi and Mombasa, offering real-time 24-hour security monitoring'.[lxxxi] The Integrated Public Safety Communication and Surveillance System (IPSCSS), including surveillance cameras, was built by Safaricom and Huawei to help security forces fight crime.[lxxxii] In June 2020, the government paid Safaricom, Kenya's largest telecommunications provider, KES1.5 billion (USD13.85 million) to maintain the IPSCSS, signalling its continued use during the first year of the pandemic.[lxxxiii] Despite this, it is unclear how this system was used to monitor social distancing rules in public spaces, and to enforce the dusk-to-dawn curfew.

In Uganda, the government continued deploying a mass surveillance system, including CCTV cameras. Uganda's integrated surveillance system uses facial recognition and other artificial intelligence systems and is also able to check vehicle licence plates and monitor social media. In November 2020, these CCTV cameras were used to track and identify individuals who participated in anti-government protests during the first year of the pandemic, resulting in their arrests.[lxxxiv]

Notably, the government insisted that its use of this integrated system helped to enforce the COVID-19 guidelines on social distancing, which clearly indicates that this system is being used beyond the original purpose of curbing crime.[lxxxv] The deployment of this mass surveillance system has led to self-censorship by individuals and media houses in Uganda under the belief that refraining from online and offline engagements is the only way to maintain online privacy and security.[lxxxvi] The arrests of individuals during protests relying on this system also affected the right to freedom of assembly and the right to protest, which is a crucial enabler of democratic societies.

Notably, the use of biometric mass surveillance systems in public spaces relying on facial recognition technologies raises particular challenges for the rights to privacy, data protection, and freedom of expression in Kenya and Uganda.[lxxxvii] Generally, biometric surveillance systems in public spaces or publicly accessible spaces are intrusive and raise challenges beyond the data protection and privacy realm as they also restrict freedom of expression and the freedoms of assembly and association. Therefore, biometric mass (untargeted or arbitrarily targeted) surveillance in public spaces or publicly accessible spaces should never

be allowed, whereas other uses of biometric surveillance should be allowed only if they pass the three-part test (legality, legitimacy, and necessity and proportionality), which should be narrowly interpreted.[lxxxviii]

Even where it is demonstrated that these systems satisfy the three-part test, guarantees under national law must be comprehensive. In the biometric surveillance context, both Kenya and Uganda lack a 'comprehensive legislative framework' for the use of biometric technologies by both public and private actors for surveillance purposes.[lxxxix] Despite the existence of protections under Kenya's and Uganda's data protection laws, these are inadequate in the biometric surveillance context.

Under Section 2 of Kenya's and Uganda's data protection laws, images and recordings of individuals are classified as personal data, which is broadly defined to mean any information, including identity data, relating to an identified or identifiable natural person in any form. Due to the sensitive personal data being collected and the ability to interfere with 'individuals' reasonable expectation of privacy in public spaces',[xc] the Kenyan and Ugandan Governments and any associated private entities are obliged to ensure that they incorporate data protection safeguards as they deploy and use these systems. While both data protection laws provide for limitations on the retention of personal data under Section 39 of the Data Protection Act (Kenya) and Section 18 of the Data Protection and Privacy Act (Uganda), both governments have failed to release specific data retention policies for these biometric surveillance systems.[xci] Further, it is unclear what type of security safeguards exist to protect personal data in biometric surveillance databases in both Kenya and Uganda.

Kenya's draft national CCTV policy focuses more on expanding the government's surveillance capabilities without providing safeguards for the protection of personal information. The policy has been criticised for threatening the rights to privacy and freedom of expression, and the freedoms of assembly and association. The draft policy proposed the installation of CCTV cameras in all public and private spaces and required that security agencies be granted 'reasonable access, connection, linkage and integration mechanisms on CCTV systems'.[xcii] The Ugandan Government has not released any draft CCTV policy for public input.

## Broad search powers to medical and public health officers

In Kenya and Uganda, public health laws grant broad search powers to medical and public health officers and inspectors to enter both public and private premises to search for, or enquire about, any cases of COVID-19.[xciii] In both countries, these powers are also granted to 'other persons acting on the written instructions of a medical officer', but it is not clear which category of persons fall under this broad term or whether these powers can be delegated to police officers.[xciv]

Strikingly, despite the broad and intrusive nature of these search powers, they are not accompanied by a requirement for a judicial warrant, which is often mandated in the context of the exercise of police search and seizure powers, to protect the rights to privacy and expression.[xcv] In this context, search warrants are granted after review by a court or independent adjudicatory body where it has been proven that reasonable and legitimate grounds exist to limit the right to privacy. While this requirement for a search warrant may be waived, this only applies in very exceptional circumstances, including 'exigent circumstances' where a police officer must act quickly. In Kenya, these powers are accompanied with a general penalty of KES20,000 (USD184.67) and imprisonment of up to six months, or both for a breach of the Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020.[xcvi]

While it is in the greater public interest to urgently contain the pandemic, granting such powers to medical and public health officers and inspectors contravenes the requirements of international human rights law and standards outlined earlier, subjecting any restrictions on the right to privacy to the three-part test. Further, there is a glaring absence in Kenya's and

Uganda's public health laws detailing the safeguards which exist to protect personal data which is collected by medical and public health officers during a search. Lastly, these public health laws fail to specify the purpose of this data collection and how the data will be processed and used, which creates opportunities for data misuse without appropriate oversight.

## Lack of transparency and accountability by state and non-state actors

The lack of transparency by state and non-state actors, and the state's failure to promote the public's right to know exacerbates fears of indefinite surveillance and data exploitation. In Kenya, government entities failed to respond to multiple access to information requests from Kenyan citizens and human rights organisations.[xcvii] In July 2020, a constitutional petition (No. 218 of 2020) detailed the Kenya Government's failure to 'proactively publish and publicise important information about the pandemic and the state's response.'[xcviii] The petition also highlighted various instances of non-compliance with Kenya's Access to Information Act, 2016 by state agencies, including the Ministry of Health, the Ministry of Interior, and the Inspector General of Kenya, amongst others.[xcix]

In Uganda, NITA-U developed a privacy policy for the COVID-19 ('Coronavirus') tracing app developed by the Ministry of Health and NITA-U;[c] however, the policy is not publicly available and accessing it on NITA-U's website requires prior authorisation.[ci] This 'prior authorisation' requirement to access a document held by a public body, which has not been classified as an 'exempt record', is not in line with the proactive disclosure of information practices under international law and Uganda's Access to Information Act, 2005. Additionally, this authorisation requirement reveals that NITA-U, where the data protection authority is housed, is not transparent and does not respect the public's right to know.

Lastly, this authorisation requirement is inconsistent with Section 8 of the Access to Information Act, 2005 which mandates public bodies to indicate how individuals or third parties can access records that are subject to automatic 'disclosure and availability' requirements. NITA-U has not responded to the project partners' formal request made on email on 15 March 2021 for a copy of the policy.

As discussed in the next section, numerous non-state actors who developed and deployed coronavirus apps were equally not transparent and accountable.

# Coronavirus apps in Kenya and Uganda

This section provides an overview of the coronavirus apps deployed in Kenya and Uganda and the impact on the rights to privacy, data protection, freedom of expression, and access to information. The issues observed include their limited impact and effectiveness, non-compliance of apps with privacy standards, inadequate privacy policies, and lack of transparency in partnerships.

## Overview of coronavirus contact tracing apps in Kenya and Uganda

Generally, coronavirus contact tracing apps rely on different location technologies, including Global Positioning System (GPS), Bluetooth, and network-based techniques to function.[cii] They also facilitate the collection of various types of personal data of individuals, including their names, ages, gender, locations, and coronavirus symptoms, among others. These aspects are detailed in Appendix 1, Tables 1 and 2.

In Kenya and Uganda, more than nine coronavirus contact tracing apps were developed by either individuals, private entities such as start-ups, or through public–private partnerships. Although the number of apps which were developed may be higher, those that were actually selected and deployed by governments are few.[ciii] In Kenya, out of the two Android apps identified in Appendix 1, Table 1 (Linda App and Jitenge MoH Kenya), only Jitenge was publicly available on the Google Play store. In Uganda, out of the two apps identified in Appendix 1, Table 2 (CovidTracer and MoH Call the Clinic [MoH CTC]), only the MoH CTC app was available on the Google Play store.

The Jitenge MoH Kenya app is a contact tracing and quarantine management app that enables contact tracing and symptoms reporting and monitoring. This app is used by the Ministry of Health's Emergency Operations Centre, which is a module of the Emergency Alert and Reporting System (EARS).[civ] This app complements the *Home Based Isolation and Care Guidelines for Patients with COVID-19*.[cv] As part of the Jitenge system, individuals in self-isolation are required to complete a daily monitoring form detailing their symptoms and temperature readings and share the information through the app. These individuals may be monitored by health care workers who feed monthly reports to the Jitenge system. These reports can be accessed by county and national rapid response teams.[cvi]

Uganda's MoH CTC app is a telemedicine healthcare app which was developed by CTI Africa, a local social enterprise.[cvii] The app is one out of eight apps developed to support the fight against COVID-19 as part of a government-sponsored initiative, the National ICT Initiatives Support Program, run by the Ministry of ICT & National Guidance.[cviii] According to the app description on Google Play, it is designed to 'ease patients' experience during a medical e-Consultation'.

In March 2020, NITA-U developed the nCov19 (Corona Virus) National Task Force Surveillance System and the COVID-19 Portal for use during the pandemic.[cix] The nCov19 National Task Force Surveillance System is a tracking and monitoring system that enables the digital registration of individuals entering Uganda, the monitoring of quarantined travellers, and the real-time reporting to the Ministry of Health about travellers' status and risk rating.[cx] The COVID-19 Portal is a response information hub that provides different actors with up-to-date and real-time information on COVID-19.[cxi] Additionally, the portal has an SMS and Unstructured Supplementary Service Data (USSD) alert system (USSD code *260#) where persons can report suspected COVID-19 cases and receive various health alerts and information, leveraging on individuals' locations.[cxii]

It is claimed that digital technologies, including coronavirus apps, offer digital solutions to tackle the pandemic whilst illustrating innovation in the ICT sphere.[cxiii] As demonstrated next, the utility and justification of these apps and 'digital/tech solutionism' generally 'as a centerpiece of infection control'[cxiv] continues to be challenged.

## Limited impact and effectiveness

To ascertain the necessity of an app, its impact and effectiveness for pandemic surveillance purposes must be measured. To this end, an app must be 'widely deployed' and used by 'at least 60% of the population',[cxv] bearing in mind that coronavirus apps rely heavily on access to digital and Internet-enabled devices (e.g. smartphones) and broadband connectivity.

In both countries, broadband access and smartphone uptake is growing but this growth has not been reflected in the uptake of the coronavirus apps.[cxvi] In Kenya, active mobile subscriptions stood at 59.8 million in June 2020, which 'translated to a mobile SIM penetration of 125.8%'.[cxvii] Smartphone uptake stood at 41%, whereas the number of individuals who own a mobile phone that is not a smartphone stood at 45% in 2018.[cxviii] In Uganda, mobile subscribers stood at 27.7 million in December 2020.[cxix] Smartphone ownership stood at 16% in 2019.[cxx]

As set out in Tables 1 and 2 in Appendix 1, it is clear that the majority of the population, currently estimated at 47.56 million (Kenya) and 40.8 million (Uganda), are not using these apps and that they failed to effectively address the pandemic during the first year.[cxxi] Kenya's app has only been installed 10,000+ times, whereas Uganda's app has only been installed 1,000+ times, as reported on the Google Play store (on 16 April 2021). Further, Uganda's over-the-top tax probably limited potential users from making use of the MoH CTC app.[cxxii]

## Non-compliance of apps with privacy standards

The project partners examined the compliance of select coronavirus contact tracing apps using Exodus Privacy's audit platform for Android apps and reviewed their description and permissions on Google Play store.

The data protection laws in Kenya and Uganda promote the principle of data minimisation which requires app developers to ensure that the number of app permissions are limited to that which is 'adequate, relevant and necessary' for a specific purpose(s).[cxxiii]

As shown in Appendix 1, Table 1, the app permissions required by the Jitenge MoH Kenya app, in relation to the description of the app, are inconsistent with its purpose, and breach the data minimisation principle. Here, out of eight permissions, four are rated as 'dangerous' or 'special' and permits the app to take pictures and videos; access location data (network-based and precise location in the foreground); directly call phone numbers; and prevent a phone from sleeping.

A similar trend was observed in Uganda where, as shown in Appendix 1, Table 2, nine out of 20 permissions are required to access and use the MoH CTC app and are rated as 'dangerous' or 'special'. These nine permissions permit the app to access location data (network-based and GPS); directly call phone numbers; take pictures and videos; read the contents of a user's external storage card; read phone status and identity; record audio; appear on top of other apps (on the system alert window); modify or delete the contents of your SD card.

From the above, it is clear that there are failures to incorporate privacy safeguards at the design stage (i.e. privacy by design) as these apps capture more personal information than is required for their stated purpose. These 'dangerous' or 'special' permissions are a data protection risk because they enable access to otherwise restricted data, including private and potentially sensitive user data, such as location and contact information, which may not be 'directly relevant to the core functionality of the app or [be] required by law'.[cxxiv] In so doing, they breach the data minimisation and purpose limitations principles under the data protection laws.

Additionally, the deployed apps also relied heavily on location data which threatens digital anonymity, which itself is fundamental to free expression. De-identification and

anonymisation are privacy techniques which, generally, transform data with the intention of permanently and completely removing both direct (name, numbers) and indirect (gender, geographical locations, date of birth) identifiers from data to prevent the identification of an individual.[cxxv] Despite this, the risk of re-identification using, for example, algorithms which can merge anonymised datasets with other identifiers such as mobile phone logs, reveals that these guarantees of privacy are not full-proof.[cxxvi]

## Inadequate privacy policies

Privacy policies are important because they detail the procedures and practices relating to the collection, processing, and storage of personal data. Typically, a comprehensive privacy policy must set out, at a minimum, a description of the organisation and the app, the type of information collected, the purpose of the data collection, the potential uses of the data collected, the legal basis for data collection, how the data is protected, how the data could be shared and used by third parties, the duration of the data retention, the data subject rights over the information collected, the safeguards protecting personal information, and the remedies following a breach.[cxxvii]

In Kenya, the Jitenge MoH Kenya app does not provide a privacy policy. The document indicated as the 'privacy policy' on the Google Play store is actually a guideline for programme implementers and policymakers, rather than their privacy policy.[cxxviii] This failure by the government and mKenya to develop and publish a specific privacy policy for the app, *prior* to collection and processing of data, demonstrates their violation of the data protection law and principles. In Uganda, the MoH CTC app provides a privacy policy which is relevant to the app. However, it is not comprehensive as it fails to clearly communicate what data is collected or secured, or the safeguards, including anonymity and encryption, which have been put in place.[cxxix]

To ensure that access to personal information is restricted to authorised personnel and to assess whether safeguards really exist, including database security, developers must disclose whether their app uses a centralised or decentralised system.[cxxx] Centralised designs create vulnerabilities, with centralisation creating a single point of failure at the point of data processing and storage. This single point of failure exposes users' personal data to hacking or exploitation by state and non-state actors and raises misuse and function creep concerns.[cxxxi] As outlined in Appendix 1, Tables 1 and 2, the design of these two coronavirus contact tracing apps in Kenya and Uganda remains unknown.

## Lack of transparency in partnerships

Both coronavirus contact tracing apps were developed by private actors, and jointly deployed in partnership with both governments. While partnerships between the government and the private sector are encouraged, these relationships must be founded on the proactive and transparent disclosure of information, including contracts, data sharing agreements, procurement documents, budgetary allocations, amongst others.

In Kenya, the Ministry of Health–mKenya partnership remains shrouded in secrecy as critical documents relating to the partnerships were publicly unavailable. Likewise the Uganda Ministry of Health–CTI Africa partnership is opaque, given the failure by both entities to publicly publish foundation documents. These transparency failures infringe on the public's right to know about the collection and use of their personal data and raises security and privacy concerns, including unauthorised access and unsupervised data sharing.[cxxxii]

# Conclusion and recommendations

This report has documented the surveillance measures and practices in Kenya and Uganda during the first year of the COVID-19 pandemic. The key trends include poor oversight over COVID-19 data collection, the lack of independent data protection authorities, the use of telecommunications data to 'track and trace' individuals, the surveillance of public spaces using CCTV and biometric technologies, the possession of broad search powers by medical and public health officers, and a lack of transparency and accountability by state and non-state actors. Also, the coronavirus apps deployed in both countries presented new challenges including their limited impact and effectiveness, non-compliance of the apps with privacy standards, their inadequate privacy policies, and a lack of transparency in partnerships.

While international human rights law and the constitutions in both countries guarantee the protection of the rights to privacy, data protection, and freedom of expression and information, these were not complied with during the pandemic period. The result is an overall expansion of the surveillance environment in Kenya and Uganda, leading to interference with, and infringements and violations of these rights, a situation which is worrying if left unchanged.

Our main recommendations to governments and private companies are as follows:

## To the governments of Kenya and Uganda

- Introduce administrative, legislative, budgetary, and practical measures to guarantee the full independence of data protection authorities.

- Introduce appropriate oversight and safeguards in public health laws, including judicial warrants, to check the broad search powers granted to medical and public health officers and other delegable officials.

- Ban biometric mass (untargeted or arbitrarily targeted) surveillance in public or publicly accessible spaces.

- Review all measures and systems deployed to address the COVID-19 pandemic which include data collection programmes, systems, and apps to ensure they strictly comply with the three-part test under international human rights law, and data protection principles, including data minimisation and privacy by design.

- Proactively disclose and make public all information and documents relating to public–private partnerships including, but not limited to, contracts, data sharing agreements, procurement documents, and budgetary allocations.

## To private companies in Kenya and Uganda

- Private entities working with the Kenyan and Ugandan Governments to develop and deploy existing and new technologies, products, and services to tackle the COVID-19 pandemic must respect human rights.[cxxxiii] In particular, they should:

  – Comply with international human rights standards, including the *UN Guiding Principles on Business and Human Rights*, and national laws protecting the rights to privacy, data protection, freedom of expression, and access to information.
  – Develop and implement comprehensive data protection measures and practices to regulate their collection, processing, and storage of personal data.
  – Integrate data protection principles, including the purpose limitation, data minimisation, data retention, and prior and informed consent, in the design, development, and deployment of technologies, products, and services to tackle the COVID-19 pandemic.

- Demand court orders before complying with government requests for individuals' data, and refuse to comply, or challenge in court, any arbitrary, unlawful, or illegal data requests or orders from government agencies or officials.
- Proactively publish transparency reports outlining the instances when user data has been requested and shared with state agencies and other private entities, the types of user data (including metadata) requested and shared, how the data was shared (compliance rates), risks to customers' data, the existing grievance mechanisms, and measures in places to protect customer data.

# Appendix 1: Coronavirus apps in Kenya and Uganda

*Table 1: Summary of two coronavirus apps (developed or deployed) in Kenya*

| **Application** | **Linda App**<br>**April 2020** | **Jitenge MoH Kenya app**<br>**June 2020** |
|---|---|---|
| **Developing/ processing entity** | • Private individuals, local | • *Developer:* mKenya, private eHealth solutions provider<br>• *Processors:* mKenya and Ministry of Health Emergency Operations Centre |
| **Type and purpose** | • Unknown type<br>• Support contact tracing effort | • Quarantine management<br>• Contact tracing<br>• Symptoms reporting app<br>• Facilitate Ministry of Health's contact tracing efforts:<br>o Home-based care management<br>o Self-quarantine<br>o Post-isolation follow-up<br>o Monitoring of long-distance truck drivers |
| **Technology used** | • Bluetooth technology<br>• Government data of individuals who had already been tested for COVID-19 and release | • Unknown |
| **Data collected** | • *Known:* phone numbers<br>• *Unknown:* biodata, etc. | • *App* (daily reminders, prompts based on mobile app)<br>• *Individuals* (self-reporting): 3 categories – air travellers, people in home isolation, and truck drivers<br><br>*Air travellers:*<br>o Name<br>o ID/passport number<br>o Country of residence<br>o Date of birth<br>o Flight details (date of arrival, flight number, seat number, destination city, email address)<br>o Telephone number in Kenya<br>o Travel history for two weeks<br>o Medical history (a list of COVID symptoms is provided)<br>o Contact information for individuals who want to enter Kenya (name of contact person and telephone, village/house number/hotel, sublocation/estate, postal address, and the county)<br>*Home isolation and truck drivers:*<br>o Country of origin<br>o Nationality<br>o Name<br>o ID/passport number |

| | | |
|---|---|---|
| | | o Physical and email address<br>o Gender<br>o Date of birth<br>o Telephone number<br>o Contact details<br>o Any additional symptomatic conditions<br>o Use of drugs/prescriptions<br>o Next of kin and their phone numbers |
| **Protection** | • Unknown | • Unknown |
| **Access** | • Google Play store (not available) | • Android mobile app (Jitenge MoH)<br>• USSD (*299#)<br>• Web-based platform |
| **Architecture (design) of app** | • Unknown | • Unknown |
| **Trackers used*** | • Unknown | • Unknown |
| **Permissions**[cxxxiv] | • Unknown | • !-Camera: take pictures and videos<br>• !-Location: network-based and precise location in the foreground<br>• !-Telephone: directly call phone numbers<br><br>*Other app capabilities:*<br>• Has full network access<br>• Views Wi-Fi and network connections<br>• !-Prevents phone from sleeping<br>• Receives data from Internet<br>• Plays Installer Referrer API |
| **Mandatory or voluntary** | • Unknown | • Two ways:<br>o Self-registration<br>o Mandatory registration by Ministry of Health or port health officials (quarantine initiation points) |
| **Database (centralised or decentralised)** | • Unknown | • Unknown |
| **No. of installs** | • Unknown | • 10,000+ |

*A tracker is a piece of software that gathers information on the person using the app, how they use it, and the smartphone being used. A tracker is usually distributed by companies as a Software Development Kit (SDK), a ready-made toolkit, aiming to make it easier for app developers. To be noted: 'open source' trackers exist; their code is available and open to everyone: https://reports.exodus-privacy.eu.org/en/info/trackers/

*Table 2: Summary of two coronavirus apps (developed or deployed) in Uganda*

| Application | CovidTracer app<br>May 2020 | MoH CTC app<br>February 2021 |
|---|---|---|
| **Developing/ processing entity** | • *Developer:* Defining Technologies (private, local)<br>• *Processor:* Donated to the Ministry of Health | • *Developer:* CTI Africa (local, social enterprise)<br>• *Processor:* funded by the Ministry of ICT; National ICT Initiatives Support Program |
| **Type and purpose** | • Contact tracing app:<br>o Tracking and identification<br>o Individuals in proximity with persons who tested positive for COVID-19 | Contact tracing and symptoms-reporting app:<br>• Deliver over the phone healthcare services<br>• Locate a patient<br>• Send community alerts about COVID-19 suspects<br>• Facilitate video and voice calls<br>• Send healthcare notifications to patients |
| **Technology used** | • Overlapping GPS (location data) and Bluetooth | • Telemedicine, AI, data<br>• Mobile team |
| **Data collected** | • Unknown | • Biodata and location data |
| **Protection** | • Unknown | • Unknown |
| **Access** | • Unknown | • Google Play store |
| **Architecture (design) of app** | • Unknown | • Unknown |
| **Trackers used** | • Unknown | • Two trackers used:<br>o Google CrashLytics (crash reporting)<br>o Google Firebase Analytics |
| **Permissions** | • Unknown | • 20 permissions:<br>• !-Location (network-based and GPS):<br>o Views network (Wi-Fi) connections<br>o Pairs with Bluetooth devices<br>o Sends sticky broadcast<br>• !-Phone: directly call phone numbers<br>• !-Camera: take pictures and videos<br>o Internet: full network access<br>o Audio settings: change your audio settings<br>• !-Read external storage: read the contents of your SD card<br>• !-Read phone state: read phone status and identity<br>• !-Record audio<br>• !-System alert window: app can appear on top of other apps<br>• Use fingerprint hardware<br>• !-Write external storage: modify or delete the contents of your SD card |
| **Mandatory or voluntary** | • Unknown | • Voluntary |
| **Database (centralised or decentralised)** | • Unknown | • Unknown |
| **No. of installs** | • Unknown | • 1,000+ |

# End Notes

i Ministry of Foreign Affairs, *Press Statement by H.E Uhuru Kenyatta*, 16 March 2020.

ii Ministry of Health, *Press Statement – Update on the COVID-19 Response in Uganda*, 13 June 2020; Uganda confirms first COVID-19 case, *The Independent,* 22 March 2020.

iii Kenya's Data Protection Act, 2019 and Uganda's Data Protection and Privacy Act, 2019.

iv Uganda Communications Commission (UCC), *Public Advisory Notice on Circulation of Fake Information*, 22 March 2020.

v Kiruti Itumi, Edgar Obare to Be Charged Under Data Protection Act – Lawyer Says, *Techweez,* 3 August 2020.

vi See: UN Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, 2011. See: OHCHR, *The Corporate Responsibility to Respect Human Rights an Interpretive Guide*, December 2012.

vii ARTICLE 19, *The Global Principles on Protection of Freedom of Expression and Privacy*, 9 March 2017.

viii The right to freedom of expression is protected by Article 19 of the UDHR, and is given legal force through Article 19 of the ICCPR (16 December 1966, UN Treaty Series, vol. 999, p. 171) and Article 9 of The African Charter, 1 June 1981. The right to privacy is protected by Article 12 of the UDHR and given legal force through Article 17 of the ICCPR.

ix UN Human Rights Council (UN HRC), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 22 May 2015, A/HRC/29/32, p. 7. See: UN HRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17 April 2013, A/HRC/23/40, para 24. See: ARTICLE 19, *The Global Principles on Protection of Freedom of Expression and Privacy*, 9 March 2017.

x ARTICLE 19's *The Global Principles on Protection of Freedom of Expression and Privacy* notes that 'data protection is essential to ensure that individuals are involved in decisions concerning their personal data and to ensure that states and companies that gather and record personal data are transparent about the data they hold; follow fair and lawful processes on the collection, use, retention, and maintenance of security of that data; and ensure that personal data collected for one purpose is not used for another.'

xi *The Global Principles on Protection of Freedom of Expression and Privacy* acknowledge the tension between the right to free expression and privacy. The Principles also recognise that 'data protection legislation can be misused or abused to prevent, end or restrict the legitimate public dissemination of accurate personal information in order to enable individuals to control their reputation at the expense of freedom of information, the right to truth and the wider public interest.'

xii ARTICLE 19, *Kenya: The Data Protection Bill*, 2019, pp. 5, July 2019.

xiii See: ARTICLE 19, *Blockchain and freedom of expression*, 2019, pp. 17. See: UN HRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35, para 5.

xiv Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*, 28 July 2014.

xv European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, Vienna, 2020, p. 20.

xvi See: UN General Assembly, *Promotion and protection of human rights and fundamental freedoms while countering terrorism*, 23 September 2014, A/69/397. See: UN HRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Martin Scheinin*, A/HRC/13/37, paras. 14–19.

xvii See: UN HRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, A/HRC/17/27, para. 24. See: Human Rights Committee, *Velichkin v Belarus*, Comm. No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

xviii See: UN General Assembly, *Resolution 68/167 The right to privacy in the digital age*, 21 January 2014, A/RES/68/167. See: UN General Assembly, *Resolution 71/199 The right to privacy in the digital age*, 25 January 2017, A/RES/71/199. See: Human Rights Watch, *Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights*, 2 April 2020.

xix ARTICLE 19, *Coronavirus apps and human rights: what you need to know*, 13 May 2020.

xx Human Rights Watch, *Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights*, 2 April 2020.

xxi Amnesty International, *COVID-19, surveillance and the threat to your rights*, 3 April 2020.

xxii UN General Assembly, *Report of the Special Rapporteur on the right to privacy*, Joseph A. Cannataci, 27 July 2020, A/75/147.

xxiii Ibid, para 46.

xxiv Ibid, para 84.

xxv Ibid, para 45.

xxvi Ibid, para 70.

xxvii Ibid, para 76.

xxviii See: UN General Assembly, *Report of the Office of the United Nations High Commissioner for Human Rights*, 30 June 2014, A/HRC/27/37, para 47. See: UN HRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17 April 2013, A/HRC/23/40.

xxix See: UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 22 May 2015, A/HRC/29/32, para 12. See: UN HRC, *Report of the United Nations High Commissioner for Human Rights*, 24 June 2020, A/HRC/44/24.

xxx UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 22 May 2015, A/HRC/29/32, para 12.

xxxi Ibid.

xxxii UN HRC, *Report of the United Nations High Commissioner for Human Rights*, 24 June 2020, A/HRC/44/24, para 24.

xxxiii See: UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 22 May 2015, A/HRC/29/32, para 12. See: UN General Assembly, *Report of the United Nations High Commissioner for Human Rights*, 3 August 2018, A/HRC/39/29, para 20.

xxxiv African Declaration on the Internet Rights and Freedoms, *Principle 8: Privacy and Personal Data Protection*.

xxxv Electronic Frontier Foundation, *Necessary and Proportionate International Principles on the Application of Human Rights to Communications Surveillance*, Principle 11: Integrity of Communications and Systems.

xxxvi UN HRC, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, 22 May 2015, A/HRC/29/32, para 56.

xxxvii ARTICLE 19, *The Global Principles on Protection of Freedom of Expression and Privacy*, Principle 4: Communications surveillance.

xxxviii UN HRC, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/13/37, para 21.

xxxix UN General Assembly, *Report of the Special Rapporteur on the right to privacy*, Joseph A. Cannataci, 27 July 2020, A/75/147.

xl ARTICLE 19 and the PROTECT Consortium, Kenya: Official Secrets Act 1970 (Revised 2012) and Amendments (2020), August 2020.

xli UN General Assembly, *Report of the Office of the United Nations High Commissioner for Human Rights*, 30 June 2014, A/HRC/27/37.

xlii See: UN HRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 16 May 2011, A/HRC/17/27, para 43. See: UN HRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35, para 2.

xliii See: Freedom House, Kenya: Freedom on the Net 2019. See: *Nation Media Group Limited & 6 others v Attorney General & 9 others* [2016] eKLR.

xliv Monitor Team, Government threatens to arrest VPN users, *Daily Monitor*, 22 January 2021. See: Stephen Kalema, Museveni orders ICT experts to find ways of blocking VPNs in Uganda, *Watchdog Uganda*, February 2021.

xlv See: UCC, *The Uganda Communications Commission Operational Guidelines on SIM Card Registration in Uganda*, 1 December 2020. See: UCC, *Reminder to Providers of Online Data Communication and Broadcasting Services to Obtain Authorisation*, 8 September 2020.

xlvi See: CIPESA, *State of Internet Freedom in Africa*, September 2019; See: Privacy International, *State of Privacy Kenya*, 26 January 2019.

xlvii See: CIPESA, *State of Internet Freedom in Africa*, September 2019; See: Privacy International, *State of Privacy Kenya*, 26 January 2019.

xlviii These regulatory policy documents (strategies and guidelines) also promote other online and offline surveillance measures such as points-of-entry-surveillance, which are beyond the scope of this report.

xlix Isaac Kadowa, *Using evidence and analysis for an adaptive health system response to COVID-19 in Uganda in 2020*, Ministry of Health: Kampala; TARSC, EQUINET, November 2020.

l One Trust Data Guidance, Uganda: NITA-U publishes tracing app privacy policy, 21 May 2020.

li UN General Assembly, *Report of the Special Rapporteur on the right to privacy*, 5 August 2019, A/74/277.

lii Government body responsible for safeguarding data protection rights through the provision of oversight, public awareness, and promotion of self-regulation.

liii Office of the Data Protection Commissioner, Office of the Data Protection Commissioner commemorates its 100th Day, 24 February 2021.

liv Section 5, Data Protection Act, 2019.

lv Section 2, Data Protection and Privacy Act, 2019.

lvi NITA-U, *Strategic Plan 2018/19–2022/23*, p. 2.

lvii European Union Agency for Fundamental Rights, *Elements of independence of the data protection authorities in the EU: Data protection authorities' funding and staffing*.

lviii Department for Digital, Culture, Media & Sport, *Explanatory Framework for Adequacy Discussions Section G: The Role of the ICO and Redress*, 13 March 2020.

lix Some issues that have not been addressed include the nominating and appointing entity/person, the director's mandatory qualifications, and term limit, amongst others. See: The National Information Technology Authority, Uganda Act 2009. See: The Data Protection and Privacy Act, 2019.

lx Section 25 of The National Information Technology Authority, Uganda Act, 2009.

lxi European Union Agency for Fundamental Rights, *Elements of independence of the data protection authorities in the EU: Data protection authorities' funding and staffing*.

lxii Here, the government attaches a surveillance officer to each patient and these officers periodically monitor the patient while in self-quarantine.

lxiii Dickens Olewe, Coronavirus in Africa: Whipping, shooting and snooping, *BBC News*, 8 April 2020.

lxiv Ibid.

lxv Mary Wambui, Kenya: Hope as Three Kenyans Develop App for Contact Tracing, *All Africa,* 17 June 2020.

lxvi Francis Monyango, Mask or muzzle: The impact of COVID-19 measures on digital rights in Kenya, in *the impact of COVID-19 on digital rights in Africa*, African Declaration on Internet Rights and Freedoms Coalition, November 2020. pp. 126–134.

lxvii "Their mobile phones are being monitored. When you swear to self-quarantine you state where you will do so. If you move (from the stated area) you are supposed to report this. You are not supposed to switch off your gadgets," said one source. See: Cyrus Ombati, State taps phones of isolated cases, *The Standard*, 24 March 2020.

lxviii MTN, MTN Uganda and NITA-Uganda launch new app for tracking COVID 19 patients under Home based care, 19 March 2021.

lxix Geofencing is a location-based service in which an app or other software uses GPS, RFID, Wi-Fi, or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a geofence. See: Sarah K. White, What is geofencing? Putting location to work, *CIO Africa*, 1 November 2017.

lxx Nathan Ernest Olupot, MTN, NITA-U Launch an App to Track & Monitor Covid-19 Patients in Home Based Care, *PC Tech Magazine,* 19 March 2021.

lxxi In Uganda, electronic point of entry screening and a travel pass were implemented at border points. See: Prosper Behumbiize, Electronic COVID-19 Point of Entry Screening and Travel Pass DHIS2 implementation at Ugandan Borders, dhis2community, April 2020.

lxxii Fred Ojambo, Uganda Orders 'Mobile Quarantine' for Truckers to Curb Coronavirus, *Bloomberg*, 29 April 2020.

lxxiii Health ministry activates electronic cargo and driver tracking system in Elegu, *The Independent*, 16 November 2020.

lxxiv SADC, *Regional Standard Operating Procedures for Management and Monitoring of Cross Border Road Transport at Designated Points of Entry and COVID-19 Checkpoints*, SADC/CM-EM/3/2020/2B, 23 June 2020, p. 1.

lxxv Tripartite of COMESA, EAC, and SADC, *Tripartite Guidelines on Trade and Transport Facilitation for the Movement of Persons, Goods and Services Across the Tripartite Region during COVID-19 Pandemic*, 29 July 2020.

lxxvi Privacy International, *Telecommunications data and Covid-19*.

lxxvii UN Department of Economic and Social Affairs (UNDESA), *Compendium of Digital Government Initiatives in response to the COVID-19 Pandemic*, 2020, p. 61.

lxxviii The privacy policy stipulates that personal data can be shared under the following circumstances: (a) by Law or to protect rights, (b) with affiliates, including government affiliated agencies involved in the fight against COVID-19 such as COVID-19 National Task Forces, and with authorised persons subject to consent.

lxxix Graham Greenleaf & Bertil Cottier. (2020). *Comparing African Data Privacy Laws: International, African and Regional Commitments*. *SSRN*.

lxxx Privacy International, *State of Privacy Kenya*, 26 January 2019.

lxxxi The Permanent Mission of the Republic of Kenya to the UN, Speech by His Excellency Hon. Uhuru Kenyatta during the 2019 State of the Nation Address at Parliament Buildings, Nairobi, 4 April 2019.

lxxxii KICTANet (Victor Kapiyo, Grace Githaiga), Kenya: Is surveillance a panacea to Kenya's security threats? In Global Information Society Watch, Communications surveillance in the digital age, 2014.

lxxxiii Edwin Mutai, State releases Sh1.5bn for Safaricom's police cameras deal, *Business Daily,* 29 June 2020.

lxxxiv Stephen Kafeero, Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests, *Quartz Africa* 27 November 2020.

lxxxv *The Independent*, Police attributes crime reduction to installation of CCTV cameras, 1 July 2020. See: *Xinhua*, Ugandan police start installation of security cameras to curb crime, 4 September 2018.

lxxxvi Tafi Mhaka, How social media regulations are silencing dissent in Africa, *Al Jazeera*, 12 November 2020.

lxxxvii These issues are canvassed extensively in ARTICLE 19's forthcoming report. See: ARTICLE 19, *When bodies become data: Biometric technologies and freedom of expression,* 2021.

lxxxviii Ibid.

lxxxix Ibid.

xc Ann Cavoukian, *Surveillance, Then and Now: Securing Privacy in Public Spaces*, pp. 23–47, June 2013.

xci Ibid.

xcii See: Ministry of Interior and Coordination of National Government, *National CCTV Policy (Draft Two)*. See: Frankline Sunday, CCTV Cameras to be Mandatory in New Law, *Standard Media,* 3 August 2019; Amnesty International, *Kenya: Desist From Indiscriminate And Invasive Mass Surveillance*, 14 August 2019.

xciii Uganda – see: *Public Health (Control of COVID-19) Rules, 2020*; Kenya – see: *Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020*.

xciv Kenya: Rule 5, *Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020*. Uganda: Rule 6, *Public Health (Control of COVID-19) Rules, 2020*.

xcv UN General Assembly, *Report of the Special Rapporteur on the right to privacy*, Joseph A. Cannataci, 27 July 2020, A/75/147.

xcvi Rule 15(1), The *Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020*.

xcvii In 2020, ARTICLE 19 Eastern Africa and other members of a coalition sent out three information requests, either directly or indirectly, to the Ministry of Interior. Out of these requests, the Ministry only responded to one.

xcviii *Erick Okioma & 12 Others vs Mutahi Kagwe, Cabinet Secretary for Health & 8 Others*, Petition No. 218 of 2020.

xcix Ibid.

c One Trust Data Guidance, Uganda: NITA-U publishes tracing app privacy policy, 21 May 2020.

ci NITA-U, Privacy Policy.

cii Privacy International, *There's an app for that: Coronavirus apps*, 20 April 2020.

ciii Kenya: Other apps and systems that were developed/conceptualised include eKonnect; KoviTrace; NTSA cashless payment platform/service for matatu/minibus users with contact-tracing features; Together Trace; and Wellvis App. Uganda: Other apps and systems that were developed/conceptualised include the Surveillance Tracing and Follow-Up System for COVID; the Symptoms Mapping and Health Care App; the Uganda Health Survey Geographical Information System; the Movement Authorisation Web-based App; the Electronic Quarantine Management System; a GIS-based Disease Surveillance System for Mbarara Hospital; and the Cogniware Insights Epidemiology App. These apps are beyond the scope of this report. See: Angela Oketch, Kenya: Covid-19 Contact Tracing Made Easy by Tech, *All Africa,* 17 January 2021. See: Joseph Muraya, Kenya: 3 Tech Firms Develop Mobile Application to Support COVID-19 Contact Tracing, *All Africa*, 12 April 2020. See: Kiruti Itumi, Kenyan Lecturer Develops App For COVID-19 Contact Tracing, *TechWeez,* 12 June 2020. See: Mary Wambui, Kenya: Hope as Three Kenyans Develop App for Contact Tracing, *All Africa,* 17 June 2020. See: Tom Phillips, Kenya to combine cashless payments with Covid contact tracing on Matatu minibuses, *NFCW,* 11, January 2021. See: James Kariuki, Safaricom among 29 tech companies licensed to offer cashless payment in matatus, *Nairobi News,* 5 January 2021. See: Mishaal Rahman, Here are the countries using Google and Apple's COVID-19 Contact Tracing API, 28 December 2020. See: European Investment Bank, Africa's digital solutions to tackle COVID-19, July 2020. See: Ugandans develop app for Covid-19 contact tracing, *Daily Monitor*, 23 May 2020. See: Utamu, Toskin Gregory, a Student at UTAMU Develops a COVID19 Tracing App, *Utamu Campus News*, 23 June 2020.

civ EARS 'provides crucial data for decision making and epidemic control measures at the national and county levels.' See: mHealth Kenya, Public Health Surveillance & Response Systems.

cv Ministry of Health, *Home Based Isolation and Care Guidelines for Patients with COVID-19*, June 2020.

cvi Reports indicate that '405,220 persons have been enrolled into the system with 332,896 at the airport traveller's module. In the same system, the Ministry has captured the details of 64,702 long distance truck drivers. About 5,985 from isolated quarantine facilities and 545 from home-based isolation and care.' See: Angela Oketch, Kenya: Covid-19 Contact Tracing Made Easy by Tech, *All Africa,* 17 January 2021.

cvii See: CTI Africa, Government launches Ministry of Health Call the Clinic (MoH CTC) mobile application, 28 May 2020. See: CTI Africa, Download MoH CTC app.

cviii Ministry of ICT & National Guidance, NIISP III Award Winners.

cix NITA-Uganda, NITA-U COVID-19 Precautionary Measures, 25 March 2020.

cx Ibid. This system is available on the website and via a mobile phone app and is allegedly only accessible by the COVID-19 National Task Force. This system is also supposed to help the Ministry of Health to electronically capture information that was previously captured manually on paper.

cxi See: Government of Uganda COVID-19 Response Information Hub. See: UNDESA, *Compendium of Digital Government Initiatives in response to the COVID-19 Pandemic*, 2020.

cxii See: Government of Uganda COVID-19 Response Information Hub.

cxiii Gary Shapiro, How innovation is helping mitigate the coronavirus threat, *Stat*, 4 March 2020.

cxiv ARTICLE 19, *Coronavirus apps and human rights: what you need to know*, 13 May 2020.

cxv Ibid. See also: Luca Ferretti, Chris Wymant, Michelle Kendall et al., Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, *Science,* 368 (6491), 8 May 2020.

cxvi Laura Silver, Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally, PEW Research Center, 5 February 2019.

cxvii Communications Authority of Kenya, *First Quarter Sector Statistics Report for the Financial Year 2020/2021 (July–September2020)*, pp. 8.

cxviii Ibid.

cxix UCC, Market Performance Report 4Q2020, April 2021.

cxx In September 2020, reports emerged that the government surveillance system was 'overstretched… affecting contact tracing and evacuation of positive cases from communities.' Here, the government affirmed that its surveillance system was only detecting '10 to 15 percent of the Covid-19 cases because contacts become too many to be efficiently followed up', which raises queries about the gaps that coronavirus apps are filling. See: Research ICT Africa, *The State of ICT in Uganda*, May 2019; See: Tonny Abet, Covid-19: Contact tracing overwhelms govt, *Daily Monitor,* 22 September 2020.

cxxi See: Kenya National Bureau of Statistics, 2019 Kenya Population and Housing Census Volume I: Population by County and Sub-County, 4 November 2019, p. 5; See: National Population Council, Key facts on Uganda's population.

cxxii NP Admin, Government urged to scrap OTT, *Nile Post*, 13 March 2021.

cxxiii See: (Kenya) Section 25(d), Data Protection Act, 2019. See: (Uganda) Section 14, Data Protection and Privacy Act, 2019.

cxxiv See: developers, Permissions on Android; See: Robert B, GDPR and Mobile Apps, 19 February 2020.

cxxv De-identification and anonymisation are often considered synonymous. However, unlike anonymised data, de-identified data 'may not necessarily be anonymized data… (which means) that the personally identifying information may be able to be re-associated with the data at a later time. In such cases, anonymized data is a particularized subset of de-identified data.' See: Educause, Guidelines for Data De-Identification or Anonymization, July 2015. See: Privacy Analytics, What is the difference between data masking, de-identification, and anonymization?, 10 June 2020.

cxxvi See: DigiTorc, Re-Identification of anonymised data sets, 10 April 2019. See: Kelsey Campbell-Dollaghan, Sorry, your data can still be identified even if it's anonymized, *Fast Company*, 10 December 2018.

cxxvii For example, the privacy policy used by the UK's National Health Service sets out these issues. See: National Health Service, NHS Test and Trace, Privacy Information, 25 February 2021.

cxxviii Lauren Spigel, Samuel Wambugu & Christina Villella, *mHealth Data Security, Privacy, and Confidentiality:Guidelines for Program Implementers and Policymakers*, MEASURE Evaluation.

cxxix CTI Africa, LifeHealth Privacy Policy. Under section 20 of the Data Protection and Privacy Act, data controllers, collectors, or processors are required to 'secure the integrity of personal data by identifying all reasonably foreseeable internal and external risks to an individual's personal data and establish safeguards against those identified risks. See: Section 20, Data Protection and Privacy Act, 2019.

cxxx 'Notifications can either be made through a centralised system, where a central authority has access to and is able to process contact information contained in all users' devices. Or it can happen through a decentralised architecture, where this information and the processing of it happens on users' devices.' See: ARTICLE 19, *Coronavirus apps and human rights: what you need to know*, 13 May 2020.

cxxxi UN General Assembly, *Report of the Special Rapporteur on the right to privacy*, Joseph A. Cannataci, 27 July 2020, A/75/147, para 73.

cxxxii Grant Goodes, Most Government-Sponsored COVID-19 Contact Tracing Apps Are Insecure and Risk Exposing Users' Privacy and Data, *Guardsquare,* 18 June 2020.

cxxxiii This list includes, but is not limited to, telecommunications and mobile network operators, coronavirus app developers and implementers, and biometric technologies developers and implementers.

cxxxiv The icon ! indicates a 'Dangerous' or 'Special' level according to Google's protection levels.