

# GLOBAL INFORMATION SOCIETY WATCH 2019

## *Artificial intelligence: Human rights, social justice and development*



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC),  
ARTICLE 19, AND SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY (SIDA)

# Global Information Society Watch

## 2019



## Global Information Society Watch 2019

Artificial intelligence: Human rights, social justice and development

### Operational team

Valeria Betancourt (APC)  
Alan Finlay (APC)  
Mallory Knodel (ARTICLE 19)  
Vidushi Marda (ARTICLE 19)  
Maja Romano (APC)

### Project coordination team

Valeria Betancourt (APC)  
Cathy Chen (APC)  
Flavia Fascendini (APC)  
Alan Finlay (APC)  
Mallory Knodel (ARTICLE 19)  
Vidushi Marda (ARTICLE 19)  
Leila Nachawati (APC)  
Lori Nordstrom (APC)  
Maja Romano (APC)

### GISWatch 2019 advisory committee

Namita Aavriti (APC)  
Rasha Abdul Rahim (Amnesty International)  
Alex Comminos (Research ICT Africa)  
Malavika Jayaram (Digital Asia Hub)  
J. Carlos Lara (Derechos Digitales - América Latina)  
Joy Liddicoat (Centre for Law and Emerging Technologies, University of Otago)  
Andrew Lowenthal (EngageMedia)  
Micaela Mantegna (Geekylegal/Machine Intelligence Lab, Center for Technology and Society, San Andres University)  
Valeria Milanés (Asociación por los Derechos Civiles)

### Project coordinator

Maja Romano (APC)

### Editor

Alan Finlay (APC)

### Assistant editor and proofreading

Lori Nordstrom (APC)

### Publication production support

Cathy Chen (APC)

### Graphic design

Monocromo

### Cover illustration

Matías Bervejillo

We would like to extend a special note of thanks to a number of authors who have made ad honorem contributions to this edition of GISWatch.

We gratefully acknowledge the following:

Philip Dawson and Grace Abuhamad (Element AI)  
Anita Gurumurthy and Nandini Chami (IT for Change)  
Rasha Abdul Rahim (Amnesty International)



APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19 for their support for Global Information Society Watch 2019.

Published by APC

2019

Printed in USA

Creative Commons Attribution 4.0 International (CC BY 4.0)

<https://creativecommons.org/licenses/by/4.0/>

Some rights reserved.

Global Information Society Watch 2019 web and e-book

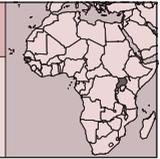
ISBN 978-92-95113-13-8

APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

Disclaimer: The views expressed herein do not necessarily represent those of Sida, ARTICLE 19, APC or its members.

# UGANDA

## “CAMERAS, MOBILES, RADIOS – ACTION!”: OLD SURVEILLANCE TOOLS IN NEW ROBES IN UGANDA



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Daniel Mwesigwa

<https://cipesa.org>

### Introduction

Artificial intelligence (AI) has dramatically changed the ways in which machines can “watch”, “listen”, “act” and importantly, “learn”; in other words, how machines can be used in the social, economic and political spheres. In this report, I discuss broadly how neural networks, deep learning and natural language processing (NLP)<sup>1</sup> – all components of AI – are deployed in Uganda by actors in the public and private sectors and international development for different purposes.

To illustrate this, I highlight three pathways of AI deployment in Uganda: the government has recently installed surveillance CCTV cameras in the capital Kampala and surrounding metropolitan areas; a large Ugandan telco is using big data to target subscribers with micro loans via mobile money; and a UN agency is mining radio content to analyse sentiment for policy and planning purposes.

While there are benign intentions and even justifications for the deployment of the aforesaid technologies in the given contexts, I highlight how their implementation might enhance the actors’ surveillance capabilities and result in the abuse of fundamental human rights such as the right to privacy.

I use the labels “big brother”, “big tech” and “big other” to represent the new surveillance tools used by the state, private sector and international development agency respectively.<sup>2</sup>

### Background

Uganda is a landlocked country in East Africa bordering Kenya to the east, Tanzania in the south, the Democratic Republic of Congo in the west and South Sudan in the north. It has a population of 37.7 million people according to the bureau of statistics.<sup>3</sup> It has a GDP per capita of USD 604 according to the World Bank.<sup>4</sup> Over 69% of the working population is employed in the agriculture sector,<sup>5</sup> which contributes 25% to the GDP.<sup>6</sup> Most notable is the rise of telecommunications and mobile telephony that have become pervasive nationwide. Internet penetration currently stands at 13.5 million subscribers, a rate of 35%, according to the Uganda Communications Commission.<sup>7</sup>

### The new Panopticon

The country has had a long reign of relative peace and stability in the past 33 years, thanks to the ruling President Yoweri Kaguta Museveni who ascended to power in 1986 after years of guerrilla warfare against the sitting governments of the time. The country has since then registered considerable socioeconomic growth but now faces the state’s growing assertiveness in managing security threats, perceived or real, and the fast-rising opposition to the incumbency. In this context, the war on terror and dissent are conveniently categorised under the rosy covers of “national security”.

A spate of extrajudicial killings and untold assassinations of high-profile Ugandan citizens, including Muslim clerics, military and police officers, among others, led the government to expedite the procurement of 24-hour CCTV cameras in crime-prone areas in Kampala and surrounding areas. The first phase of installation comprised 1,940 cameras

1 In *AI Superpowers*, Kai-Fu Lee explains that neural networks work based on the amount of test data fed to them, upon which the networks themselves identify patterns within the data. Deep learning entails more efficiently trained layers in neural networks. Deep learning’s most natural application is in fields like insurance and loans, where relevant data on borrowers is abundant (credit score, income, recent credit card usage), and the goal to optimise the use of this data is clear (i.e. to minimise default rates). Both terms could be used interchangeably for the first two CCTV and micro loans examples. Lee, K. (2018). *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin Harcourt.

2 Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. Shoshana Zuboff frames the tension about big tech’s overtures as “surveillance capitalism”, where users and even non-users are surveilled largely for commercial purposes. In this article, I use big tech and big other independently of each other.

3 UBOS. (2014). National Population and Housing Census 2014. <https://www.ubos.org/onlinefiles/uploads/ubos/NPHC/CENSUS%20FINAL.pdf>

4 <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UG>

5 <https://data.worldbank.org/indicator/SL.AGR.EMPL.ZS?locations=UG>

6 <https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS?locations=UG>

7 [https://twitter.com/UCC\\_Official/status/1088826901702078466](https://twitter.com/UCC_Official/status/1088826901702078466)

in the capital in 2018.<sup>8</sup> However, the planned second phase will cost the public purse over USD 104 million in a procurement deal rushed through parliament under unclear terms.<sup>9</sup>

### The alchemists

As fable goes, alchemists of yesteryear tried to reverse engineer precious metals through a combination of different elements. However, most of their efforts were in vain. Today, mobile operators are the new alchemists. Just like the alchemists, telcos are collating precious registration data alongside other data that would have been considered useless decades ago (when machine learning was not as advanced as today). They have mastered the art of extracting value out of this mix of data.

Telcos have benefited immensely from government regulation and the loopholes in regulation. For example, the mandatory SIM card registration in Uganda entailed the collection of biometric data and personally identifiable information in spite of a lack of sufficient constitutional guarantees on data protection and privacy. The evidence shows that the main reason for this mandatory registration – crime – has not been fully addressed, if at all.<sup>10</sup>

This kind of registration data, supplemented through often opaque data agreements with data brokers, is the juicy stuff that telcos – and others – are leveraging to build deep-learning models for their product offerings. For example, MTN Uganda in partnership with IBM rolled out a mobile loans programme on the country's largest network. IBM uses customer and economic data to model customer behaviour and risk. They have built credit scoring models based not only on MTN's data but also on national identity card data. This sort of targeting has become so precise that telcos and tech giants like IBM are not just the new alchemists, extracting value *ex nihilo*, but also “surveillance capitalists”.

### The “benign” surveillance of radio

In Uganda, radio is the most pervasive form of media. There are over 117 radio stations today<sup>11</sup>

– up from only one in the 1990s. More than 400 licences have been granted to FM radio operators. At least 98% of the population listen to radio once in a year. Contrasted against other forms of media such as newspapers (100,000 copies circulated per week), TV and the new kid on the block, the internet (13.5 million subscriptions), radio's reach remains unmatched.

However, there has been so little innovation happening in the radio space that even broadcasting radio over the web could well pass as groundbreaking. In this context, the UN Global Pulse's radio analysis tool promises much.<sup>12</sup> It is an NLP machine that identifies key words which are then analysed to determine “sentiment” and enable the UN to chart advocacy efforts or even policy interventions. Good intentions aside, there are pertinent questions that the radio content analysis tool raises, and which possibly might open a can of worms, especially when it comes to bias or data abuse.

### Big Brother Uganda

The Constitution of Uganda emphasises that the government through its agencies must guarantee security of persons and property. The issue of national security gives the government powers among other things to surveil, monitor and intercept communications, and track movement as it deems fit, in order to secure the country's territorial integrity against internal and external aggression. Through different enforcement mechanisms, the government's mandate to facilitate state surveillance is enabled by the following select laws: the Anti-Terrorism Act, 2002; the Regulation of Interception of Communication Act, 2010; the Anti-Pornography Act, 2014; the Communications Act, 2013 (amended 2017); and the Data Protection and Privacy Act, 2019.<sup>13</sup>

The ubiquity of mobiles and motorcycles (also known as *boda bodas*) marked the turn of the last decade in Uganda. Both have been used to do as much good as they have been used to do harm. For example, they have enabled last-mile communication and cheap transport to hard-to-reach places such as rural areas. But a great deal of the runaway crime in the country that pre-empted mandatory SIM card registration among other interventions by the government was committed by hitmen using un-registered mobiles and *boda bodas*.

8 The Independent. (2019, 15 April). More than 1900 CCTV cameras installed in Kampala. *The Independent*. <https://www.independent.co.ug/more-than-1900-cctv-cameras-installed-in-kampala>

9 Misairi, T. K. (2019, 26 April). Uganda: MPs Okay Shs386b Loan for City Spy Cameras. *AllAfrica*. <https://allafrica.com/stories/201904260210.html>

10 Wanyama, E. (2018, 18 April). The Stampede for SIM Card Registration: A Major Question for Africa. *CIPESA*. <https://cipesa.org/2018/04/the-stampede-for-sim-card-registration-a-major-question-for-africa>

11 Kalyegira, T. (2013, 31 December). 20 years of FM radio stations in Uganda. *African Centre for Media Excellence*. <https://acme-ug.org/2013/12/31/20-years-of-fm-radio-stations-in-uganda>

12 <https://www.unglobalpulse.org/projects/radio-mining-uganda>

13 <https://www.ulii.org/ug/legislation/act/2015/2002>; <https://ulii.org/ug/legislation/act/2015/18-2>; [www.ug-cert.ug/files/downloads/The-Anti-pornography-act-2014](http://www.ug-cert.ug/files/downloads/The-Anti-pornography-act-2014); [parliamentwatch.ug/wp-content/uploads/2016/10/The-Uganda-Communications-Amendment-Bill-2016.pdf](http://parliamentwatch.ug/wp-content/uploads/2016/10/The-Uganda-Communications-Amendment-Bill-2016.pdf); <https://ulii.org/ug/legislation/act/2019/1>

The government's installation of CCTV cameras in the city and surrounding areas is an attempt to curb the spate of assassinations and urban crime, at least according to Museveni.<sup>14</sup> However, there is little to write home about. The high-profile killings continue episodically.

At least one expert has warned that the government intends to adopt more uncanny approaches to address infrastructural deficits including using facial recognition.<sup>15</sup> A government which said it was buying a "porn machine" to monitor and track pornography online (it denied this later), and which then silently deployed an Intelligent Network Monitoring System (INMS) on mobile operators' infrastructure, is surely capable of surreptitiously deploying any technology as long it justifies the end.<sup>16</sup> Evidence in countries that have poor human rights records such as Ethiopia, Angola and Zimbabwe shows how governments are rushing to secure facial recognition to manage "traffic" and foster "social cohesion".<sup>17</sup> Uganda is no exception.

## Big tech

Mobile telecommunications are an essential mark of communications in modern society including the developing world. The advancements in value-added services means that value is no longer confined to traditional offerings such as voice/text and data. In fact, ancillary services such as mobile money are said to be the future of mobile operators. With the growth of targeted approaches through deep learning, MTN Uganda and IBM debuted a mobile loan application dubbed "MoKash".<sup>18</sup> Other telcos such as Airtel Uganda, microfinance institutions and shiny upstarts have launched related programmes; however, MTN's offering is noteworthy because it has scale, reach and first-mover advantage.<sup>19</sup>

MoKash utilises subscribers' usage patterns and histories to weight appropriate credit scores. As mentioned, this is then coupled with biometric data from the national ID database.

Deep learning tools employed by the telco are extractive technologies; for example, they are efficient in nudging subscribers to take micro loans which attract exorbitant annualised repayment rates. But since the learning happens within the telco's ecosystem without knowledge of extant factors such as a customer's participation in the informal economy, the loans algorithm potentially leaves out subscribers who would have otherwise qualified. Others, meanwhile, are manipulated into taking loans to satiate a craving rather than out of necessity. The massive troves of data collected by telcos are subject to abuse. The complex web of players in the black market who offer data brokerage services is growing wider by the day.

## Big other

Following the privatisation of the economy in the early 1990s, radio emerged as a medium of choice for many wishing to enter the media sector. It is available in the majority of spoken languages in Uganda. But radio station ownership is dominated by political and religious groups. These circumstances mean that state actors, especially security agencies and the communications regulator, have kept radio programmes under their cross-hairs despite considerable development of other forms of mass media such as broadcast television and the internet.

It is not uncommon to find unsuspecting people intently listening to radio especially on *boda bodas* or in local public places. More than 25,000 people call in to radio stations every day. Local programming is hyper localised and often entails relevant grassroots political and educational talk shows. Meanwhile, there are known lobby groups of radio callers in Uganda that corral and attempt to influence conversation on topics *du jour*.

The public nature of radio means that people do not provide their consent when data processors such as the UN Global Pulse's radio tool are used.<sup>20</sup> The automated speech recognition tool listens to dozens of radio stations simultaneously, flags relevant content when specific keywords are mentioned and generates transcripts for deeper analysis.<sup>21</sup>

14 New Vision. (2018, 9 October). Museveni commissions CCTV cameras. *New Vision*. [https://www.newvision.co.ug/new\\_vision/news/1487292/museveni-commissions-cctv-cameras](https://www.newvision.co.ug/new_vision/news/1487292/museveni-commissions-cctv-cameras)

15 An ICT policy expert interviewed for this article warned that the adoption of facial recognition for the CCTV project could be in the offing.

16 Mwesigwa, D. (2016, 26 August). Uganda's 'Pornography-Blocking Machine' Appears To Be Part Of A Darker Censorship Agenda. *iAfrican*. <https://www.iafrican.com/2016/08/26/ugandas-pornography-blocking-machine-appears-to-be-part-of-a-darker-censorship-agenda/>

17 Gwagwa, A., & Garbe, L. (2018, 17 December). Exporting Repression? China's Artificial Intelligence Push into Africa. *Council on Foreign Relations*. <https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa>

18 <https://www.mtn.co.ug/en/mobile-money/banking/Pages/mokash.aspx>

19 Cambridge Centre for Alternative Finance, & MicroSave. (2018). *Fintech in Uganda: Implications for Regulation*. [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2018-ccaf-fsd-fintech-in-uganda.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-ccaf-fsd-fintech-in-uganda.pdf)

20 Muhangi, K. (2019, 4 March). Overview of the data protection regime in Uganda. *New Vision*. [https://www.newvision.co.ug/new\\_vision/news/1495211/overview-protection-regime-uganda](https://www.newvision.co.ug/new_vision/news/1495211/overview-protection-regime-uganda)

21 Rosenthal, A. (2019, 18 April). When old technology meets new: How UN Global Pulse is using radio and AI to leave no voice behind. *United Nations Foundation*. <https://www.unglobalpulse.org/news/when-old-technology-meets-new-how-un-global-pulse-using-radio-and-ai-leave-no-voice-behind>

However, some particular audio segments are queued for human review.<sup>22</sup> Upon analysis, the local government or the UN can gather insights that help inform policy decisions.

The tool is tuned to the central and northern regions of the country, where the Luganda and Luo languages are, respectively, widely spoken (there are over 41 spoken languages in Uganda, according to Ethnologue, which geographically limits the tool's coverage).<sup>23</sup>

While the radio tool adheres to UN privacy and data protection principles, these principles might not be aligned with the laws of the land, particularly the Data Protection and Privacy Act, given that the national laws are often in flux.<sup>24</sup> This potentially could create a diplomatic rift if data is used for purposes that are effectively illegal according to the national data laws.

## Conclusion

In this article, I have highlighted three pathways of actual and expected AI deployment in Uganda. We now have the big brother, big tech and big other – the state, private sector and an international development agency respectively.<sup>25</sup>

The government has taken steps to combat threats, real and imaginary, through procurement of advanced technology, among other measures. Chiefly, the procurement of CCTV cameras has raised concerns on data protection and privacy. The infrastructural deficiencies (poor or no street lighting, limited connectivity, low standards of maintenance) undermine potential benefits. However, the state is expected to use AI facial recognition technologies to arbitrarily deal with persons of interest including dissidents. The lack of trust, openness and transparency that shrouds state-led interventions impacts on society negatively. For example, the unexplainable leakage of footage from CCTV cameras in Kampala raises questions on ethical standards and requirements to manage the retrieval, sharing and erasure of public CCTV footage.<sup>26</sup>

“It’s now imperative that government engages with citizens on these [surveillance] tools,” a respondent to this report said. “We’re not talking about the future we want to see. We perhaps do not want facial recognition at this stage.”

African writer and political analyst Nanjala Nyabola in a *Financial Times* article said “using technology as a substitute for trust creates this black box. But most of us don’t understand how these [AI] systems are built. So what comes out is just chaos.” Nanjala also said that telcos are at the stage of a “mass data sweep” in which data about an expanding consumer class is being busily devoured. In our context, big tech products such as MoKash are examples of the extraction and commodification of user data.

Meanwhile, machine learning is not as advanced as we might think. Most of it is labour and sweat. For example, the UN’s Global Pulse radio tool methodology is laborious and subject to false positives – it is fraught with problems such as changes in the accents of callers and so-called “serial callers” who regularly phone in to radio stations to support a party, meaning that the data is not representative of the reality on the ground.

The enactment of the Data Protection and Privacy Act in Uganda in February 2019 is a positive step, given that it coincides with an aggressive push for CCTV camera installation and other activities that engender massive data sweeps. While the law has not yet been operationalised, it is important that the state fast tracks its implementation. The responsible state actors should ensure compliance and high ethical standards for data processing, especially in the cases covered in this report.

The government needs big tech – and big other – to help it understand what legislation and policies, including oversight and enforcement mechanisms, are necessary to strengthen the protection of human rights in the rapidly changing digital world.

We have been led to believe that data is the new oil.<sup>27</sup> Instead, we should be challenged to think of meaningful ways we could collectively participate in the data economy where privacy, security and profit are all held in high regard.

22 An ICT policy respondent interviewed for this article raised concerns about the opacity of the radio tool methodology. They say that transcription is manual. There is no automatic voice-speech synthesis.

23 <https://www.ethnologue.com/country/UG/languages>

24 United Nations Development Group. (2017). *Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda*. [https://undg.org/wp-content/uploads/2017/11/UNDG\\_BigData\\_final\\_web.pdf](https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf)

25 Although the private sector and development world might have closer overlaps, and therefore the “big otherness” might be used loosely and interchangeably.

26 <https://twitter.com/dispatchug/status/1121455937724788736>

27 Mwesigwa, D. (2019, 8 April). Is data really the new-found oil? *Daily Monitor*. <https://www.monitor.co.ug/OpEd/Letters/-data-oil-World-Wide-Web-Google-search-digital/806314-5061646-ghfmesz/index.html>

## Action steps

The following are the overarching action steps for civil society:

- Civil society, media and academia, among others, should unpack the conversations on AI and re-frame them in digestible and locally relevant ways.
- Civil society should work hand in hand with the government to fast track the implementation of the recently passed data protection and privacy law.
- It should contribute to the regular reviews of laws to keep them in line with rapid advancements in technology, particularly AI.
- It should advocate for best and ethical design practices for AI products and services.
- It should act as a watchdog with regard to potential abuses of fundamental human rights through deployment of AI technologies by different actors.

## Author's postscript

On 15 August 2019, *The Wall Street Journal* published an investigative piece called “Huawei Technicians Helped African Governments Spy on Political Opponents”. The article detailed how Huawei had helped the Ugandan police infiltrate encrypted communication channels used by an opposition leader. Notably, it also mentioned Uganda’s plans to open a new six-storey USD 30 million hub in November 2019, which will be linked to the over USD 104 million “Smart Cities” project implemented by Huawei. The project includes surveillance using CCTV cameras equipped with Huawei facial-recognition technology.<sup>28</sup> This information was not in the public domain at the time of writing of this country report. However, the report remains valid and prescient.

---

28 Parkinson, J., Bariyo, N., & Chin, J. (2019, 15 August). Huawei Technicians Helped African Governments Spy on Political Opponents. *The Wall Street Journal*. <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>

# Artificial intelligence: Human rights, social justice and development

Artificial intelligence (AI) is now receiving unprecedented global attention as it finds widespread practical application in multiple spheres of activity. But what are the human rights, social justice and development implications of AI when used in areas such as health, education and social services, or in building “smart cities”? How does algorithmic decision making impact on marginalised people and the poor?

This edition of Global Information Society Watch (GISWatch) provides a perspective from the global South on the application of AI to our everyday lives. It includes 40 country reports from countries as diverse as Benin, Argentina, India, Russia and Ukraine, as well as three regional reports. These are framed by eight thematic reports dealing with topics such as data governance, food sovereignty, AI in the workplace, and so-called “killer robots”.

While pointing to the positive use of AI to enable rights in ways that were not easily possible before, this edition of GISWatch highlights the real threats that we need to pay attention to if we are going to build an AI-embedded future that enables human dignity.

GLOBAL INFORMATION SOCIETY WATCH  
2019 Report  
[www.GISWatch.org](http://www.GISWatch.org)

