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 Comninos (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 Milanes (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)

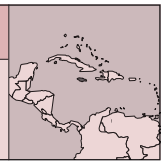
APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19
for their support for Global Information Society Watch 2019.

Published by APC
2019
Printed in USA

Global Information Society Watch 2019 web and e-book
ISBN 978-92-95113-13-8
APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

JAMAICA

ARTIFICIAL INTELLIGENCE AND "CONSENT OF THE GOVERNED": PITFALLS IN DEVELOPING JAMAICA'S DIGITAL ID SYSTEM



Mona ICT Policy Centre (MICT), The University of the West Indies
Hopeton S. Dunn
https://conf.carimac.com/index.php/cybersecurity/2019

Introduction

In a recent landmark ruling, Jamaica's Chief Justice Brian Sykes observed that the government's harsh decision to impose criminal sanctions to enforce compulsory registration by all citizens in a new digital ID system was a remarkable choice "in a democracy where the exercise of executive power rests upon the consent of the governed."[1]

This report discusses the government's planned use of artificial intelligence (AI) to create a new national identification system (NIDS) as a unique verifier of every Jamaican citizen. The enabling legislation, called the National Identification and Registration Act (NIRA), was approved by Parliament in 2018 under the leadership of the Andrew Holness-led government. It was presented as a means of modernising and integrating a clutch of existing national ID data sources, including census data, tax registration metrics and electoral roll data. Loan funding to the tune of USD 68 million was being provided by the Inter-American Development Bank (IDB) to acquire the supporting AI technology, and to roll out information campaigns and other implementation services related to the nationwide capture of biometric data for machine classification, analysis and storage.

While the overall plan for a national ID system was widely deemed as an important advance for the country's development, there were some elements of the plan that generated deep public concern and became the basis of a legal challenge by the parliamentary opposition. These included the highly intrusive level of biometric data being demanded, the compulsory nature of the plan, criminal sanctions for non-compliance, and the absence of adequate safeguards for data protection. The scenario that emerged by 2019 was one in which AI was being used to undermine the privacy rights, personal choices and constitutional freedoms of an entire population.

In April 2019, the Jamaican Supreme Court largely agreed with the expressed concerns and handed down a historic ruling, designating the new NIRA law "null, void and of no effect."[2]

Legislative context

Jamaica is a parliamentary democracy that gained political independence from Britain some 57 years ago, in 1962. Since then, two major political parties, the currently ruling Jamaica Labour Party (JLP) and the opposition People's National Party (PNP), have alternated power, both claiming strong affinity to democracy and the rule of law. The apex of the judicial system is still the United Kingdom Privy Council, but the country's Supreme Court, headed by an independent chief justice, serves as the top court of original jurisdiction. The Supreme Court includes a constitutional division.

Jamaica's independence constitution was amended with bi-partisan support in April 2011 to include a Charter of Fundamental Rights and Freedoms, which established or strengthened a range of key citizen protections. Among other provisions, the Charter specifies that "Parliament shall pass no law and no organ of the state shall take any action which abrogates, abridges or infringes the guaranteed rights." These rights include the "right to equitable and humane treatment by any public authority in the exercise of any function"; the "right to protection from search of the person and property" without a warrant; "respect for the protection of private and family life, and privacy of the home"; and "protection of privacy of other property and of communication".[3]

There are as yet no legal provisions in Jamaican law conferring specific protections against the ill effects or misuse of AI systems. However, a March 2010 Cybercrimes Act addresses computer-specific offences, such as unauthorised access to computers

1 Chief Justice Sykes, Para 23 of the Supreme Court Ruling on the National Identification and Registration Act. supremecourt.gov.jm/content/robinson-julian-v-attorney-general-jamaica

2 Supreme Court of Jamaica. (2019). Ruling of Full Court in Claim Number 2018HCV01788 between J. Robinson, Claimant and the Attorney General of Jamaica, Defendant. supremecourt.gov.jm/content/robinson-julian-v-attorney-general-jamaica

3 https://japarliament.gov.jm/attachments/341_The%20Charter%20of%20Fundamental%20Rights%20and%20Freedoms%20(Constitutional%20Amendment)%20Act,%202011.pdf

and illegal data alteration. Amendments to the Act in 2015 offered additional protections as well as stiffer penalties for cybercrime offences.[4] However, a key companion piece of legislation, the Data Protection Act,[5] though in draft form since 2017, has not yet been debated and approved by Parliament. In this regard, the start of the collection of people's biometric data under provisions of the NIRA in 2018 was deemed by some observers to be premature and troubling.

NIRA, biometrics and the court

The NIRA was approved in the Jamaican Parliament in December 2018 over the strong objection of sections of civil society and the parliamentary opposition. The law made formal registration by all citizens compulsory and required them to provide specific biometric information on pain of criminal sanctions. A central registering authority, created by the Act, was mandated to collect identity verifiers, including iris scans and fingerprints and using facial recognition technologies. However, in a departure which many citizens and the parliamentary opposition deemed unwarranted and extreme, the Act also required the capture of vein patterns, and if needed, footprints, toe prints, palm prints and the blood type of citizens and residents. The compilation and analysis of these biometrics were to be executed using big data analytics and pattern recognition technologies.

The new law specified that "(e)very person who refuses or fails, without reasonable excuse, to apply to the Authority for enrolment in the database... commits an offence and shall be liable on conviction to the penalty specified." The government refused to accede to demands made by civil society and the parliamentary opposition for changes, or even to extend the public and parliamentary debate time before final approval. As a result, the NIRA law was referred by the opposition to the Supreme Court for a ruling on the constitutional validity of certain key sections.

The court's ruling was delivered on 12 April 2019 in a 309-page judgment, from a panel of three judges, led by Chief Justice Sykes. In his written judgement, the chief justice paid particular attention to the compulsory nature of the law and its recourse to criminal sanctions for non-compliance:

> Here we see the ultimate coercive power of the state being enlisted to ensure compliance – the risk of imprisonment even if the risk is reduced. The learned Attorney General contended that when you have a system of compulsory registration then there has to be a means of enforcement that may be an effective method of ensuring compliance. The policy choice, it was said, was to use the criminal law. This response by the learned Attorney General suggests that persuasion was not thought to be a reasonable option, a seemingly remarkable conclusion in a democracy where the exercise of executive power rests upon the consent of the governed.[6]

At the end of the detailed written ruling, the judges of the Supreme Court announced that the legislation violated numerous sections of the Charter of Fundamental Rights and Freedoms of the Jamaican constitution. It found that data collection methods and the protocols of intended data use did not sufficiently guarantee respect for and protection of privacy, and that there were insufficient safeguards against the misuse and abuse of the data to be collected.

So riddled was the legislation with what the court deemed unconstitutional clauses, that the judges said they were obliged to disallow the entire NIRA law. Accordingly, the court ruled unanimously that the entire NIRA was "null, void and of no effect."[7]

In the event, Jamaica's first attempt to use AI on an extensive basis for public data gathering and analysis was deemed unconstitutional on the grounds of inadequate attention to the civic, personal, legal and social implications of the Act. According to one commentator, the government had "promoted the transactional value of the technology, rather than the fundamental value of the principles for which it was adopted."[8] In an editorial, the Gleaner newspaper also remarked:

> The Supreme Court's comprehensive slap-down of the government's national identification law has implications beyond the need of the Holness administration to reflect deeply on its future approach to the formulation of laws. For it raises questions, too, about our commitment to the Constitution.

The newspaper reminded readers that part of the haste in passing this legislation was related to "the need to meet the Inter-American Development Bank's funding cycle for a US$68 million loan for the project."[9]

4 https://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf

5 https://www.japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202017----.pdf

6 Supreme Court of Jamaica. (2019). Op. cit.

7 Ibid.

8 Morris, G. (2019, 14 April). Jamaica's NIDS setback of its own making. *Jamaica Observer*. www.jamaicaobserver.com/the-agenda/jamaica-s-nids-setback-of-its-own-making_162161?profile=1096

9 The Gleaner. (2019, 16 April). Editorial – NIDS Ruling Breaks New Ground. *The Gleaner*. jamaica-gleaner.com/article/commentary/20190416/editorial-nids-ruling-breaks-new-ground

A large part of those loan funds would have been used to acquire the AI technology that would have been embedded in what the law called the National Civil and Identification Database (NCID).

Identity, AI and cyber risks

The proposed new national database in Jamaica was to be a prime site for big data analytics in an emerging global technology environment. According to the Harvard Business Review, the technologies that enable AI, like development platforms and vast processing power and data storage, are advancing rapidly and becoming increasingly affordable. Yet it warns that the successful deployment of AI requires a deliberate policy of "rewiring" the organisation involved in its utilisation. AI initiatives, it argues, face formidable cultural and organisational barriers if not carefully deployed.[10]

In a similar vein, digital security analyst Sarah Vonnegut says special measures are often needed to safeguard AI-generated and other digital databases. She argues that databases that are important to companies and government organisations are very attractive to hackers and can be vulnerable to numerous forms of attack. One vulnerability is the so-called "buffer overflow" vulnerability, when a programme "tries to copy too much data in a memory buffer, causing the buffer to 'overflow' and overwriting the data currently in memory." Vonnegut says buffer overflow vulnerabilities "pose an especially dangerous threat to databases holding particularly sensitive info, as it could allow an attacker exploiting the vulnerability to set unknown values to known values or mess with the program's logic."[11]

Dana Neustadter, from the internet content design company Synopsys, says secure algorithms are a large part of the value of any AI technology:

> In many cases, the large training data sets that come from public surveillance, face recognition and fingerprint biometrics, financial, and medical applications, are private and often contain personally identifiable information. Attackers, whether organized crime groups or business competitors, can take advantage of this information for economic reasons or other rewards. In addition, the AI systems face the risk of rogue data injection maliciously sent to disrupt neural network's functionality (e.g., misclassification of face recognition images to allow attackers to escape detection). Companies that protect training algorithms and user data will be differentiated in their fields from companies that suffer from the negative PR and financial risks of being exploited.[12]

In the absence of adequate data security safeguards, it is clear that the extremely sensitive biometric data that were to be collected to create the NIDS in Jamaica would have been especially vulnerable to these and other forms of malicious attack, without legal recourse to a modern data protection act.

While recognising the importance of applying AI and other data-related technologies to create a reliable national database, the merit of the Jamaican Supreme Court ruling is its insistence that the process not threaten citizen rights, freedoms and privacy and that better safeguards be introduced to mitigate the risks to citizen data.

Conclusion

Jamaica now faces the challenge of how to reform and re-establish a national identification system that is within the bounds of the constitution. The new successor legislation has to ensure respect for citizens' rights to make informed choices about the data being collected and held. While AI will doubtless aid any renewed data gathering effort, care will be needed to ensure robust data protection, secure and reliable data storage and overall data integrity on the principles laid down, for example, by the 2018 General Data Protection Regulation (GDPR) of the European Union.[13] Jamaica's own long-pending Data Protection Act will need to be debated and enacted as a matter of priority, and to precede any data collection under any revised ID law.

Against the background of the Supreme Court ruling, the compulsory provisions and criminal sanctions will have to be removed in favour of greater stakeholder consultation, public education and what the Chief Justice calls citizen "persuasion". The intrusive nature and unwarranted details required in the biometric data being sought from citizens will also have to be reviewed to provide for citizen consent and the provision of advance justification on the part of government for the collection of each type of sensitive biometric data.

10 Fountaine, T., McCarthy, B., & Saleh, T. (2019). Building the AI-Powered Organization. *Harvard Business Review, July-August*. https://hbr.org/2019/07/building-the-ai-powered-organization

11 Vonnegut, S. (2016, 24 June). The Importance of Database Security and Integrity. *Checkmarx*. https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database-security-and-integrity

12 Neustadter, D. (n/d). Why AI Needs Security. *Synopsys*. https://www.synopsys.com/designware-ip/technical-bulletin/why-ai-needs-security-dwtb-q318.html

13 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Action steps

The following steps are necessary in Jamaica:

- It must be recognised that establishing a national ID system is not the sole responsibility of the government; it is necessary that civic, academic, human rights and corporate stakeholders become more involved in hosting public forums on AI, human rights and national ID systems.
- The government itself should re-commit to a thorough legal and policy review in line with the requirements imposed by the Supreme Court ruling. Any new national ID legislation must benefit from extensive public consultations and wider parliamentary deliberations.
- A significant proportion of the loan funds committed to this project by the IDB should be devoted to public education, citizen consultations and to ensure data protection and integrity.
- International case studies on the establishment of successful national ID systems should be produced by the relevant government agencies and used to inform a process of public education towards a new AI-assisted national ID system for Jamaica.
- Finally, the outcomes and recommendations of the 7th National Cyber Security Conference, which was hosted by the Mona ICT Policy Centre at the University of the West Indies in June 2019, need to be made more widely available to government and all other stakeholders.[14]

14 https://conf.carimac.com/index.php/cybersecurity/2019

GLOBAL INFORMATION SOCIETY WATCH 2019

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

APC
ARTICLE 19
Sida