

GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

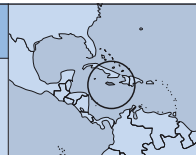


ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Creative Commons Attribution 3.0 Licence <creativecommons.org/licenses/by-nc/3.0/>



The University of the West Indies

Hopeton Dunn and Allison Brown
www.mona.uwi.edu

Introduction

A recent Supreme Court ruling in Jamaica prohibiting a state agency from gaining access to the telephone data of Jamaican citizens touches on several of the international principles of human rights in relation to surveillance. In the case, Supreme Court judge Justice Ingrid Mangatal ruled in June 2013 that telecommunications provider Digicel was not compellable under the law to provide customer data or subscriber information to the investigative state agency called the Independent Commission for Investigations (INDECOM). In this report we analyse the circumstances of this ruling and the implications regarding constitutional protections in Jamaica and the Caribbean against unauthorised surveillance by government of the personal data of citizens.

Background

Jamaica is a small independent, English-speaking country in the Caribbean. The most recent census in 2011 tallied a population of just below 2.7 million.¹ The country operates a bi-cameral parliament with a bill of rights and a constitution that emphasises democracy and the rule of law.

Jamaica's GDP per capita was reported by the Planning Institute of Jamaica in 2010 to be USD 4,979.² Services such as tourism and information and communications technologies (ICTs) remain key contributors to GDP, with traditional products such as bauxite, sugar and bananas playing important roles in employment and GDP output. The current National Development Plan, named Vision 2030, targets developed country status by 2030.

ICTs are a central aspect of the national development plan as they are seen as a growth industry in their own right as well as a driver of economic and social development. A 2011 survey indicated that 94% of the population were mobile phone users, 16% of households had internet access, while 45%

of individuals used the internet from anywhere.³ These indicators would have moved upwards significantly since that survey, particularly in the area of mobile broadband usage. The cost of equipment and services is the key hindrance to the growth of the online population in Jamaica.

Policy context

The telecommunications and ICT industry is mainly governed by the Telecommunications Act of 2000, which was amended in 2011. This is supplemented by other pieces of legislation such as the Electronic Transactions Act of 2007 and the Cybercrimes Act of 2010. Key legislation in relation to state surveillance is applied in the Interception of Communications Act of 2002 (amended in 2011) while section 47 of the Telecommunications Act speaks to the protection of customer data by telecommunications service licence holders. Jamaica's Charter of Human Rights (2011) addresses the right of everyone to privacy of property and of communication. Despite longstanding calls from civil society and the academic community, a Data Protection Act is still in the consultation stage, now promised for introduction to parliament sometime in 2014.⁴ This act would protect the privacy of citizens' personal data and would regulate the "collection, processing, keeping, use and disclosure" of such data.⁵

Basics of the case

As we thematically consider the issue of communication surveillance in the digital age, the Jamaican case of *Digicel (Jamaica) Limited v The Independent Commission of Investigations*⁶ is of special interest. The case touches on many of the international principles of human rights in relation to surveillance. The matter arose from a request for informa-

1 STATIN. (2012). *Population Census Data*. Kingston: STATIN.

2 Planning Institute of Jamaica. (2012). *Jamaica Country Assessment (Preliminary Draft)*. Kingston: PIOJ.

3 Dunn, H., Williams, R., Thomas, M., & Brown, A. (2011). *The Caribbean ICT and Broadband Survey Jamaica*. Mona: Telecommunication Policy and Management Programme, University of the West Indies.

4 The Data Protection Act will possibly reflect model legislation developed by the ITU-led Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR). www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx

5 Angus, G.L. (2014, June 11). Laws far advanced to modernize ICT sector. *Jamaica Information Service*. jis.gov.jm/laws-far-advanced-modernize-ict-sector

6 [2013]JMSC Civ. 87.

tion from police monitoring agency INDECOM to dominant telecom provider Digicel in 2011 for call origination data. This data was to have been used in the investigation of the shooting death of Robert “Kentucky Kid” Hill in 2009 at the hands of members of the local security forces. Digicel brought the case to the Jamaican Supreme Court against INDECOM in order to clarify their responsibilities in the sharing of customer data. In summary, the outcome was a Supreme Court ruling which prohibited the state agency INDECOM from gaining access to the telephone data requested.

Digicel (Jamaica) Limited v The Independent Commission of Investigations

Digicel (Jamaica)

Digicel Jamaica is the first telecommunications provider which entered the Jamaican market after its liberalisation in 2000. Prior to that, the market was controlled by the monopoly of Cable and Wireless, which now trades as LIME. Since Digicel’s entry a few other firms have entered and left the market, the most recent being Claro (América Móvil), which was acquired by Digicel in 2011. According to a survey completed in 2011, Digicel controlled, at that time, 88% of the mobile market.⁷ Its gains in market share following its acquisition of Claro have not yet been quantified, but Digicel is considered, in legal terms, to be the dominant player in the Jamaican mobile market, with LIME being the only other major player. In 2014 Digicel operates in 32 markets in the Caribbean, Central America and Asia-Pacific.

INDECOM

INDECOM conducts “investigations concerning actions by members of the Security Forces and other agents of the State that result in death or injury to persons or the abuse of the rights of persons; and for connected matters.”⁸ It was put in place by the INDECOM Act of 2010 which replaced the Police Public Complaints Act. INDECOM was to be an independent body set up to investigate injustices carried out by members of the security forces in Jamaica. This is within the context of long-held perceptions of police corruption among the wider society, including what has been seen as “many shooting incidents which have led to the death or serious injury of citizens.”⁹

A commentary in the *Western Mirror* by Robert Dalley earlier this year noted:

In some cases, there are clear facts to substantiate the claim that the person who was shot and killed by the police was brutally murdered, however, because of the fact that the country has corrupt police officers in the force and an under-performing court and judicial system, the police are not prosecuted or charged in any way.¹⁰

The *Digicel v. INDECOM* judgement refers to information from the Bureau of Special Investigations (BSI) stating that from 1999 to 2010, 2,257 persons were killed by the police (an average of 188 per year). Similar statistics have been reported by the local human rights lobby group Jamaicans for Justice. It is useful to point out that the figures indicated do not include the number of these killings which have been investigated and seen as justified by the legal system.

The *Digicel v. INDECOM* case also speaks to several attempts on the part of the local government to address the quandary of police killings and other abuses. Previous attempts include the Police Public Complaints Authority (PPCA) and the BSI mentioned above. However, while the PPCA was under-resourced, underfunded and lacked the needed authority to investigate, there was an ostensible issue of independence as it related to the second team – the BSI – which was located within the Jamaica Constabulary Force (JCF), one of the bodies the unit was required to investigate.

INDECOM was established as a resolution to these issues. The INDECOM Act of 2010 sought to bestow sufficient powers for the Commission to investigate corruption within the security forces. What can be surmised from the preceding section is that at the centre of the establishment of INDECOM is a pursuit of improved human rights practices, particularly in relation to greater accountability among security forces, the investigation of police killings and other alleged abuses by members of the security forces.

The context for INDECOM

The matter of police accountability is a subject which cannot be broached in a vacuum. We are required to highlight the high levels of major crime in Jamaica as a possible contributor to the high levels of police killings. With 1,200 murders committed

7 Dunn, H., Williams, R., Thomas, M., & Brown, A. (2011). Op. cit.

8 indec.com.jm/about_us.htm

9 *Digicel (Jamaica) Limited v The Independent Commission of Investigations* [2013] JMSC Civ. 87.

10 Dalley, R. (2014, February 2). ‘We need to reduce police killings in Jamaica’. *Western Mirror*. www.westernmirror.com/index.php/permalink/6659.html

in 2013,¹¹ the country has the sixth highest murder rate worldwide.¹² The punishment of execution for capital crimes, although on the books, has not been implemented since 1988. Some police and citizens alike have supported the idea that extrajudicial killings can be justified within the context of controlling major crimes and containing the murder rate. This is the context within which the high number of police killings must be understood.

Details of the case

This case emerged specifically from a request made on 28 September 2011 by INDECOM to Digicel requiring the telecom provider to furnish data on telecommunication services for particular subscribers who had been named in an investigation being undertaken. In the investigation of the death of Hill, the allegation emerged that his shooting was the result of a conspiracy between some named members of the security forces, a cousin of the deceased and another named female. The data was needed for further investigation of this alleged conspiracy. A parallel request was also made to LIME, the contents of which have not been discussed in detail in the judgement. Digicel noted that while it was not unwilling to provide the information, guidance would be needed from the local courts as to what is required of the telecom provider in response to the request from INDECOM. This is particularly in light of other legislation which governs such interactions. LIME, on the other hand, has complied with the request.

INDECOM cited section 21 of the INDECOM Act in its request for the data. A part of section 21 reads:

The Commission may at any time require any member of the security forces, a specified official or any other person who in its opinion is able to give assistance in relation to an investigation under this act, to furnish a statement of such information and produce any document or thing in connection with the investigation that may be in the possession of that member, official or other person.

Section 16 of the Interception of Telecommunications Act was also seen by INDECOM to be supportive of its case, where subsection 2 states:

11 Walker, K. (2014, January 1). 2013 bloodier than 2012. *Jamaica Observer*. www.jamaicaobserver.com/news/2013-bloodier-than-2012_15716666

12 Jamaica Observer. (2014, April 1). Jamaica has 6th highest murder rate worldwide – UN report. *Jamaica Observer*. www.jamaicaobserver.com/latestnews/Jamaica-has-6th-highest-homicide-rate-worldwide---UN-report

Where it appears to the designated person that a person providing a telecommunications service is or may be in possession of, or capable of obtaining, any communications data, the designated person may, by notice in writing, require the provider- (a) to disclose to an authorized officer all of the data in his possession or subsequently obtained by him; or (b) if the provider is not already in possession of the data, to obtain the data and so disclose it.

Digicel considered the requirement to provide information to be at odds with section 47 of the Telecom Act, which reads: “Every carrier and service provider shall, subject to subsection (2), regard and deal with as secret and confidential, all information regarding the type, location, use, destination, quantity and technical configuration of services used by their customers.” While exceptions are cited, none of them include that such information can be legally provided to INDECOM. The section does, however, allow for the delivery of such information “for the purpose of the investigation or prosecution of a criminal offence.” Further, the Interception of Communications Act was not seen by Digicel to compel them to furnish the data since INDECOM is not a named “authorized officer”.

In the write-up of the judgement, Justice Ingrid Mangatal noted that Digicel could not be compelled by INDECOM to provide this information as it would be in contravention of section 47 of the Telecom Act and the law cannot force a party to commit a criminal offence. There was also the issue as to whether discretion of the provider could be triggered in this case on the basis of section 47 of the Telecom Act. However, given that the documentation provided by INDECOM did not specify that the information was required for the investigation of a *criminal offence*, it was noted that the discretion of the provider could not be applied.

INDECOM has since challenged this outcome and the case is likely to return to court sometime in 2014.

Case analysis

Our understanding of this case is that the judgement does not prohibit state surveillance, but such surveillance could not be applied in the current case. If INDECOM had been named as an “authorized officer” in the Interception of Communications Act (or some amendment thereof), Digicel would have been compelled to provide whatever information INDECOM had requested. If the request had been worded differently (specifying it was needed to investigate a criminal offence), then Digicel

would have been able to provide the information at their discretion. This certainly raises concerns regarding implications for private citizens whose information could be at risk based on these possible amendments. However, these matters can only be considered in relation to the ostensible purpose of INDECOM, which at its foundation is seen as a preserver and defender of human rights and not an agency in opposition to such rights.

This case touches on many of the International Principles on the Application of Human Rights to Communications Surveillance.¹³ Jamaica continues to uphold the main understanding that value should be placed on the privacy of individuals, and simply because the state can access communications data does not always mean that the state should access such data. There are clearly boundaries and exceptions which are applied, and in the case of *Digicel v. INDECOM*, there is no major opposition to data being provided where there is a “legitimate aim” and adequate “need”. The challenge which faced the Independent Commission was that the laws had not been updated to ensure that the body was able to legally compel telecommunications providers to furnish subscriber data. Discretionary action was also eliminated as a possibility in this case because of the wording of the request to Digicel, and the omission of information which would have made compliance with the request legal.

The key outcome which must be considered is the way in which legislation lags behind developments in the telecoms sector and the gaps in understanding the ever-transforming digital age within which we operate. This is true for telecom practitioners, legal persons, law enforcement and ordinary citizens.

There is also the matter that both major telecom providers who are in control of telecommunications data are non-Jamaican entities which may also be subject to the laws of the countries in which they were initially established and countries where they operate. The role of such entities in preserving the human rights of citizens should be explored,

particularly where communication between countries can be easily monitored in one country or the other. This is of even greater concern given our understanding, through the Snowden case, that it is not necessarily the content of communication which may be monitored but also the metadata and broader patterns of communication.

The relevant matters of user notification, transparency and public oversight are emergent issues which should be tackled in the pending Data Protection Act.

Conclusions and action steps

There remains a general concern that legislation lags behind developments in the telecoms and ICT sector. This case shows one such example. Serious consideration needs to now be given to the powers which the state wishes to grant INDECOM, and to all relevant legislation that needs to be updated. These considerations are to be made in relation to human rights implications as well as to acceptable exceptions to privacy in line with the international context.

The second recommendation has to do with training and capacity building at all levels, so that practitioners and ordinary citizens alike will be able to understand the many issues at work in communications surveillance.

While the state remains a key area for consideration when it comes to communications surveillance, it is critical to contemplate how citizens, companies and foreign countries can also use communications surveillance to violate human rights. Countries like Jamaica need to ensure that legislation is robust and adequate for these threats in meeting national objectives and protecting citizens’ rights.

Finally, the Data Protection Act, which will be under parliamentary consideration in the near future, needs to take into account the International Principles on the Application of Human Rights to Communications Surveillance. In addition, it is also necessary to rationalise the new act with all relevant existing legislative and policy frameworks.

¹³ <https://en.necessaryandproportionate.org/text>