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

URUGUAY

Penumbra: Surveillance, security and public information in Uruguay

DATA
Fabrizio Scrollini
www.datauy.org

Introduction

In July 2013 a local newspaper revealed that the Uruguayan government had purchased secret surveillance software called "El Guardián".[1] El Guardián (or The Guardian) is a radical shift towards online and phone surveillance, and the challenges it represents remain largely out of public debate. This report aims to analyse the most recent developments in terms of the use of technology for surveillance in Uruguay. It will provide a description of key events and regulations that have recently emerged in Uruguay, analysing challenges to privacy. Finally it will provide a set of issues to develop an agenda for privacy according to the International Principles on the Application of Human Rights to Communications Surveillance.[2]

Government surveillance in the Uruguayan context

Uruguay is considered a stable and relatively transparent democracy by several indicators available, including that offered by Transparency International.[3] Uruguayan democracy was regained from military rule in 1985, but the country's democratic tradition goes as far back as the beginning of the 20th century, when Uruguay was one of the few democratic nations in Latin America. During the past military dictatorship (1973-1985) the Uruguayan government ran extensive surveillance programmes in order to monitor its citizens. According to the weekly publication *Brecha*, a former intelligence officer revealed that the dictatorship managed to develop profiles of at least 300,000 Uruguayans.[4] Access to these files is still contested in Uruguay, but increasingly they are becoming available to people who were under state surveillance.

Uruguay has recently being portrayed as a liberal and progressive country. In the last five years it has passed laws legalising same-sex marriage, abortion and the cultivation and sale of cannabis. Furthermore, Uruguay passed a law on free and open source software which requires that the government use free and open source software in all its activities. Regulations in line with this law are still to be developed so that it can be implemented. Montevideo City Hall was one of the leading city governments in advancing open source and open data policies in the country.

Uruguay set up a monopoly in terms of internet provision run by the state-owned telecommunications company ANTEL.[5] ANTEL is implementing a wide-ranging programme to provide internet access through optic fibre to the whole country. Previously ANTEL had secured connectivity across the country and established a scheme to provide basic access to the internet for every citizen. Today, 58% of the population has direct access to the internet, and 18% of Uruguayans are frequent internet users.[6] Furthermore, the establishment and development of the Ceibal programme has allowed every child in Uruguay access to devices (i.e. netbooks) to connect to the internet in their schools, homes and also public squares. Ceibal is fostering a new kind of education which relies heavily on the internet. In the next 10 years a new generation of digital natives with full access to computers and the internet will emerge in Uruguay.

The country has a strong judiciary system with a long tradition of upholding the rule of law. Uruguay also has a relatively strong privacy law, although there is no systematic evaluation of its implementation. Nevertheless, technological change has outpaced the capacity of government watchdog institutions to keep an eye on several developments emerging, mostly in the areas of security and defence. Most of these developments are justified

1 Terra, G. (2013). Gobierno compró "El Guardián" para espiar llamadas y correos. *El País*. www.elpais.com.uy/informacion/gobierno-compro-guardian-espiar-llamadas-correos.html

2 https://en.necessaryandproportionate.org/text

3 www.transparency.org/country#URY

4 Sempol, D. (2008). Article in *Brecha*, 16 May, cited in Zabala, M., & Alsina, A. (2008). *Secretos Publicos*. Montevideo: Fin de Siglo, p. 46.

5 Administración Nacional de Telecomunicaciones: www.antel.com.uy

6 El Observador. (2013, April 3). Uruguay a la cabeza de Latinoamérica en penetración de internet *El Observador*. www.elobservador.com.uy/noticia/247366/uruguay-a-la-cabeza-de-latinoamerica-en-penetracion-de-internet

in public discourse as new tools to fight organised crime and possible external threats, as well as to improve policing services through technology. The Uruguayan government, similar to governments in many other Latin American countries, is under heavy pressure to deal with security issues, most notably street crime. In this context there are three developments that offer a set of challenges to privacy and democracy:

- The purchase and use of digital technology (software) to potentially spy on the civilian population.[7]
- The development of surveillance systems using CCTV cameras and drones to foster public safety and better policing.[8]
- The development of a cyber-crime law which effectively outlaws a set of behaviours considered "dangerous" and limits liberties in the digital age.[9]

The aforementioned developments are taking place in a context of a lack of regulation and understanding of a number of human rights issues on the part of the authorities, the judiciary *and* institutions defending human rights.

The Guardian: Software for surveillance

In July 2013, the local newspaper *El País* broke the news about the secret purchase of The Guardian software by the Uruguayan government.[10] The Ministry of Home Affairs (*Ministerio del Interior)*, which is responsible for security issues, classified this purchase as secret under the access to information law, hiding it from official records. There was no tender as it was a direct and exceptional purchase. The cost of the software licence was USD 2 million and there is a yearly service fee of USD 200,000. The Guardian is a system designed to monitor several networks, allowing up to 30 people to work simultaneously on mobile phones, landlines and emails. The software was designed by a Brazilian company called Digitro Tecnologia. Uruguay has recently passed a "free software" law, which essentially suggests that the government should use free or open source software unless a good justification exists. The Guardian does not comply with this regulation as it is proprietary software.

According to *El País*, Digitro also provides services to the Brazilian Federal Police. In Brazil there has been intense debate about the use of The Guardian. The army and the police in Brazil openly admit that they use the tool.[11] Several accountability agencies are worried about the extent to which the software is being used on its civilian population and how exactly several state units at the national and state level are using it.[12] For instance, there were concerns that it was used in the context of the last Confederations Cup football tournament in Brazil, and the social unrest that erupted in a number of cities. Privacy Latam, a specialised blog dealing with surveillance in Latin America, reports that according to General José Carlos dos Santos from the Brazilian Army's Centre for Cyber Defence, "the monitoring is legal and justified on the grounds of national security policies and actions." He also claims that the software is adapted and customised by the user and is not used to monitor citizens in general, and that it was "used only during the 2013 Confederations Cup."[13]

In Uruguay, the authorities have reassured the media that the surveillance software will be used within the traditional legal framework, which implies that the judiciary would need to authorise surveillance activities. In the words of the Secretary of the Presidency of the Republic: "This system will centralise surveillance through telecommunications and will provide more guarantees to subjects during this process. The technology is much more advanced than we currently have in Uruguay. But we are going to keep using [as required] an order from a competent judge or a request from the public solicitor, with the consent of the telecommunications operator. Guarantees remain in place."[14]

Since then the media and the government have been relatively silent about the use of The Guardian. While the assurances that there will continue to be a legal framework that respects basic liberties and due process are comforting, there are serious challenges ahead. There are still no regulations con-

7 Terra, G. (2013). Op. cit.

8 El País. (2014, April 21). Así vuelan los colibríes de la Policía uruguaya. *El País*. www.elpais.com.uy/informacion/asi-vuelan-colibri-drones-ministerio.html

9 Presidencia de la República. (2014, June 30). Ejecutivo remitió al Parlamento proyecto de ley que pena los delitos cibernéticos. *Presidencia de la República*. www.presidencia.gub.uy/comunicacion/comunicacionnoticias/seguridad-informatica-proyecto-ley

10 Terra, G. (2013). Op. cit.

11 Lobo, A. P. (2013, July 17). Exército usou software Guardião para monitorar redes sociais. *Convergência Digital*. wap.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34302&sid=11#.U5ZMmS9htbo

12 Veja. (2013, May 6). Conselho do MP investiga uso de grampos por promotores. *Veja*. veja.abril.com.br/noticia/brasil/conselho-do-mp-investiga-uso-de-grampos-por-promotorias

13 Monteiro. (2014, February 13). Brazil monitors protests against the 2014 World Cup. *Privacy Latam*. www.privacylatam.com/?p=200

14 Portal 180. (2013, July 30). Gobierno: Guardián centraliza vigilancia electrónica pero mantiene garantías. *Portal 180*. www.180.com.uy/articulo/34766_Gobierno-guardian-centraliza-vigilancia-electronica-pero-mantiene-garantias

cerning the specific use of this tool for intelligence gathering by authorities. Currently Uruguay is in the middle of a discussion about how to structure security and intelligence services and as a result the use of these kinds of technologies is poorly regulated. At the same time, the triangulation of data collected through different security services such as the new CCTV system in place and drones is a matter of worry. A set of key questions emerge:

- How will this complex set of surveillance technologies be deployed? What is the protocol for deploying them and will it reflect the proportionality and necessity principles?
- What are the basic accountability arrangements for security officers operating these technologies?
- How will Uruguayan agencies cooperate with other intelligence agencies around the world and the region, and to what extent?

Another set of questions emerge about how the current privacy laws apply in this setting. There is a need to rethink privacy in the context of surveillance of communications, particularly where private information is held, and for how long Uruguayan authorities will be able to hold this information.

The fact that this software was purchased using a secret procedure with no parliamentary control or the involvement of other oversight bodies shows that it is necessary to rethink the accountability arrangement in this sector. Furthermore, while the Ministry of Home Affairs argues that the software is auditable, there is no specification of how it is auditable, who would perform such an audit, and whether the results of these audits are going to be available to the public.

Conclusion

The debate about surveillance, intelligence gathering and privacy is ill-informed in Uruguay. Authorities are reacting to a regional and global trend to use software to monitor telephone calls and networks for security purposes with no clear guidance or strategy (at least known to the public) that reflect human rights concerns. While public reassurances about upholding the rule of law are a good sign, the complexity of the matter calls for better regulation and engagement with civil society organisations and human rights institutions, in order to work on a human rights approach to surveillance in an age of technological change. The Uruguayan government and civil society organisations are not prepared to have a proper debate on the matter yet. On the other hand, due to its tradition of upholding the rule of law, Uruguay presents an opportunity to foster appropriate and proportionate regulation in this field.

Action steps: A call for a human rights-centred vision of security in the digital age

Denying the challenges that the state faces in an age of transnational crime is foolish and irresponsible from a citizen's perspective. But granting "carte blanche" to government authorities for surveillance with no restrictions is equally irresponsible. Uruguay has a history of less technologically developed but equally damaging surveillance during the 1973-1985 dictatorship. Until now, the release of these files and access to the records for people who were under surveillance remain problematic. In the context of a progressive democratic society, as Uruguay portrays itself, it is time to have a serious debate about privacy and security in the digital age.

The following steps are recommended to advance a human rights-centred agenda on this topic:

- Foster dialogue about principles for the use of The Guardian and other surveillance technologies between human rights institutions (such as the Ombudsman), the intelligence community and civil society, to identify common ground on this issue.
- Define clear protocols to use these tools and clear lines of accountability for public officials involved in the surveillance process.
- Define clear lines of democratic accountability and transparency on surveillance processes involving the parliament, the Ombudsman and civil society. In particular, establish a minimum of transparency around surveillance activities and a yearly report open to public scrutiny.
- Review the current privacy law and identify gaps and best practices in the context of surveillance and security activities. Consider progressive frameworks in terms of data retention and access to data for people potentially subject to surveillance.
- Promote the use of auditable (ideally open source or free software) technologies to manage data retention and secure critical data for intelligence and surveillance activities.

For a democratic society, the way forward implies allowing access to knowledge around surveillance activities, as well as keeping agencies in check when these technologies are developed. The aforementioned recommendations are the starting point for much-needed dialogue and debate on these issues in Uruguay.