Fundación
Karisma

Fundación Karisma's response to call for input to a report on the right to privacy in the digital age by the UN High Commissioner for human rights

April 9th, 2018

Hereby, Fundación Karisma (hereinafter Karisma) welcomes the opportunity to provide input to the UN High Commissioner for human rights regarding the right to privacy in the digital age. Karisma is a Colombian digital rights NGO that works in the defense of freedom of expression, privacy, access to knowledge and due process on digital spaces through research and advocacy. Karisma has worked with diverse communities, including librarians, journalists, persons with visual disability, and women's rights advocates to strengthen the defense of human rights in digital spaces. Karisma often works jointly with other NGOs and networks that support their actions and projects.

Karisma wants to raise the attention of the UN High Commissioner regarding the state of the right to privacy in Colombia. The past years have been marked by scandals involving a now defunct intelligence agency, the abuse of interception of communications capabilities and the lack of clear legislation on those issues. Most of the faculties of communications surveillance are given by administrative decree and are surprisingly vague. Therefore, there is a need to adapt the national legislation to the standards set by the International Covenant on Civil and Political Rights and the American Convention on Human Rights signed by Colombia.

As the current government period is ending, the Ministry of ICTs and other agencies are developing policies that rely heavily on the collection, processing and exploitation of data, being unclear how much of it is possible to classify as personal. Those policies are being passed without proper public discussion.

The following response is numbered according to the call issued.

2. Surveillance and communications interception:

a. Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.

The interception of communications in Colombia is regulated primarily by the Constitution, the **Criminal Procedure Code (CPC)** and a number of intelligence laws. The Constitution

empowers the Office of the Attorney General (Fiscalía General) to "[c]onduct searches, house visits, seizures and interceptions of communications" subject to judicial control (Article 250 CPC).

The CPC allows the Attorney General to conduct interception of communications for the purpose of evidence collection for crime investigation. The execution of interception is subject to judicial approval after it is done.

On the other hand, **Intelligence Law (Law 1621 of 2013)** stipulates that intelligence and counter-intelligence activities "include monitoring the electro-magnetic spectrum". Article 4 of the Law provides that information may only be obtained for a lawful purpose. Those purposes are: ensuring national security; sovereignty; territorial integrity; the security and defence of the nation; the protection of democratic institutions and the rights of Colombian residents and citizens; and the protection of natural resources and economic interests of the nation. Such broad and vaguely defined purposes allow for an expansive interpretation of the instances in which communication surveillance can be undertaken, failing to meet the tests of legality, necessity and proportionality.

Article 17 of the Law is entitled "Monitoring the Electromagnetic Spectrum and Intercepting Private Communications" and states:

"Intelligence and counter-intelligence activities include monitoring the electromagnetic spectrum when this is duly established in operational orders or work assignments. Information gathered during such monitoring in the context of intelligence and counter-intelligence activities that does not serve to achieve the aims established in this Law shall be destroyed and may not be stored in intelligence or counter-intelligence databases. Monitoring does not constitute interception of communications.

Intercepting private mobile or land-line telephone conversations, as well as private data communications shall be subject to the requirements established in Article 15 of the Constitution and the Criminal Procedure Code and may only be conducted in the context of legal proceedings."

The term 'monitoring' the electromagnetic spectrum is not defined anywhere in the Colombian law. Without any definition provided, 'monitoring' the electromagnetic spectrum could include analyzing and monitoring e-mails, text messages and phone calls that are carried upon the electromagnetic spectrum. Those acts constitute 'interception' of the communication and thus interfere with the privacy of the person sending and receiving the information.

The second paragraph states clearly that the interception of communications is not authorised by the Intelligence Law, but rather must only occur under the lawful authority of the Criminal Procedure Code, on a targeted basis, in accordance with the procedures stipulated in the Code. Nevertheless, this assertion leads to a significant legal loophole that raises serious concerns related to the protection of the right to privacy. This loophole in the law is particularly problematic given the kind of surveillance technologies employed by the

Colombian security and law enforcement forces. As noted in the Concluding Observations on the Seventh Periodic Report of Colombia released under the auspices of the UN Human Rights Committee, there are concerns that “instances in which private communications conveyed via the electromagnetic spectrum are intercepted without the benefit of a rigorous assessment of the legality, necessity and proportionality of such interceptions”.

Indeed, a report published by Privacy International in August 2014[1] set out the logical inconsistencies in the government's interpretation of the Intelligence Law as relates to electromagnetic spectrum monitoring and lawful interception.

Finally, in January 2017, a **National Code of Police and Coexistence (Código Nacional de Policía y Convivencia para Vivir en Paz)** entered into force. The new code expands police powers through a number of provisions designed to "solve the conflicts that affect the coexistence" of Colombians. It includes several provisions that have particularly negative implications with regards to the right to privacy and their collective interpretation, which can lead to a state of surveillance. These include article 163 of the Code, which states that the police can enter without a court order a private or public establishment, under conditions including certain emergencies. The provision has since been challenged in court.

Moreover, Article 327 contains an unduly narrow definition of privacy. By defining the right to privacy as the right of people “to meet their needs and develop their activities in an area that is exclusive and therefore considered private”, the provision seems to confuse the right to privacy with the right to unhindered development of personality as well as with the right to the inviolability of the home. Therefore, by linking the right to privacy with the existence of private physical spaces, it excludes from privacy protection any person or assets (such as cars, or electronic devices like portable computers or cellphones) placed in public places, including bars, restaurants, etc, while also leaving in a legal grey area private acts that may take place in a public space.

Conversely, Article 139 defines public space in a very broad way, including notably “the electromagnetic spectrum”. The combined result of these definitions is of significant concern to the protection of privacy, particularly when considering that Article 237 could be interpreted to mean that communications travelling through the electromagnetic spectrum would be excluded from privacy protection.
Lastly, the new Police Code does not seem to take into consideration the complex technological changes which affect modern communication. Hence, it is unclear how the privacy of digital communications and of online spaces is protected given the very restrictive definitions of privacy and public space included in the Code.

This shortcoming of the law was raised by the Human Rights Committee which highlighted concerns that the new Policy Code defines “the concept of ‘public areas’ in a very broad sense that includes the electromagnetic spectrum, and by the fact that all the information and data gathered in public areas are considered to be in the public domain and to be freely accessible (art. 17)”.

[1] https://privacyinternational.org/node/991

Bulk and network interception

The nation's most visible communications interception system is Esperanza (Sistema Esperanza); it is heavily supported by the US Drugs Enforcement Agency (DEA). The Office of the Attorney General (Fiscalía General de la Nación, 'Fiscalía') manages and administers the platform, which can obtain mobile and fixed-line call data and content. Esperanza, to which various law enforcement agencies have access, is connected to the nation's telecommunications operators. It is used to obtain evidence for judicial prosecution on a case-by-case basis. It requires that a Fiscalía agent physically request that an individual phone line or record be intercepted. Other safeguards built in to the Esperanza system include an electronic warrant submission system and supervisory judges (jueces de control de garantías). However, a Privacy International investigation showed, Esperanza suffered from various security vulnerabilities and its restriction to accessing data only for pre-defined individual targets on the basis of a warrant was a point of friction for other law enforcement agencies.

The Police Directorate of Criminal Investigation and Interpol (Dirección de Investigación Criminal e INTERPOL, 'DIJIN') has built the Single Monitoring and Analysis Platform (Plataforma Única de Monitoreo y Análisis, 'PUMA'), a phone and internet monitoring system linked directly to the service providers' network infrastructure by a probe that copies vast amounts of data and sends it directly to DIJIN's monitoring facility. PUMA is capable of intercepting and storing potentially all communications that pass through its probes. Communications service providers know of its existence and cooperated in its installation but are excluded from its day-to-day operation. The PUMA system is outlined in a Privacy International report.

PUMA was acquired in 2007 using technology from Israeli surveillance company Verint Systems Ltd and maintained by Compania Comercial Curacao de Colombia, a Colombian firm. In 2013, the Police put forward proposals to extend the system, claiming that an expanded PUMA would be capable of capturing three times more phone calls and data. The expanded PUMA was to include a monitoring module for internet service providers (ISP) and up to 700 workstations throughout the country. The contract for the expansion was concluded with NICE Systems, another Israeli surveillance company, in partnership with Colombian company Eagle Comercial. Yet disagreement between the Fiscalía and the Police over its management stalled the expansion, and the project was put on hold. Nonetheless, new contracts are still being settled and the revamped system was supposed to be operational by the end of 2015. It is unclear as to the current situation.

Additionally, the Police Intelligence Directorate (Dirección de Inteligencia Policial, 'DIPOL') acquired and deployed its own mass, automated communications surveillance system, the Integrated Recording System ('IRS'). Established in 2005, the IRS monitors massive communications traffic across E1 lines and 3G mobile phone traffic. Like PUMA, it is set up with service providers' knowledge and monitoring is done without their knowledge. Privacy

International's analysis of the technologies is that the system is capable of collecting 100 million call data records per day and intercepting 20 million SMS per day. This vast data store is then processed and combined with other types of data including images, video, and biometric details.

The technologies underpinning both the DIPOL and DIJIN systems automatically collect and store communications data passively via a set of probes linked to a monitoring centre. Nevertheless, whilst Decree 1704 (2012) requires telecommunications providers to set-up their infrastructure to enable “access and traffic capture” for crime investigation purposes, there is no explicit provision which either permits or prohibits measures of bulk surveillance as PUMA in the current legal framework which regulates the surveillance of communications in Colombia.

b. Role of business enterprises in contributing to, or facilitating government surveillance activities

Businesses have an important role as providers of surveillance capabilities which are meant to be used in the context of the mentioned legal framework.

IMSI Catchers

Many companies offer IMSI catcher mobile surveillance devices in Colombia, according to a Privacy International investigation. New Zealand-based Spectra Group via Colombian company Maicrotel Ltda provided its Laguna IMSI catcher to DIPOL in September 2005. The Laguna system is designed to monitor and record telephone conversations and data in mobile communication systems and could be mobile or assembled in fixed stations. Bulldog and Nesie, manufactured by UK surveillance company Smith Myers, are two other popular IMSI catchers sold in Colombia. In 2010, the DAS was preparing to purchase a Bulldog interception system for over US$ 250,000 and a Nesie system for over US$ 320,000. The Fiscalía was also planning to buy a Bulldog system for just over US$ 280,000 as was the sectional division of DIJIN in Bogotá. In 2014, the Finnish branch of Canadian telecommunications company Exfo exported its NetHawk F10 IMSI catcher to Colombia.

Intrusion malware and hacking

Hacking Team, an Italian company, produces an intrusion system that was acquired by the Colombian police. The company’s Remote Control System (RCS) can be used to hijack computer and mobile devices while remaining undetectable to users, as it is designed to bypass common antivirus programmes and encryption. By infecting a target’s device, the RCS suite can capture data on a target’s device, remotely switch on and off webcams and microphones, copy files and typed passwords. In 2014, Hacking Team had a Colombia-based field engineer and an active contract with the Colombian police. The Colombian government’s use of offensive Hacking Team malware products had been suspected since researchers at the Citizen Lab identified a command and control server for the RCS suite in Colombia. Hacking Team supplied its technology to the DEA, which

according to internal emails[2] was reportedly using the spyware to conduct surveillance from the U.S. embassy in Bogotá.

A 2014 investigation by the Citizen Lab at the University of Toronto[3], concluded that since 2012 those technologies have been identified and associated with attacks on journalists, activists and human rights defenders, and showed evidence confirming suspected deployment of those technologies in at least 21 countries, including Colombia.

Hacking Team also had two projects with the Colombian police, one of which appears to relate to the PUMA surveillance system.

The Colombian army has also employed hackers, as revealed in the Andromeda spying scandal. The army also trains cadets to hack in the Army Intelligence and Counterintelligence School (Escuela de Inteligencia y Contrainteligencia), as seen by Privacy International.

4. National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particular business enterprises, related human rights protection gaps and ways to bridge those gaps.

Data Retention

For the purpose of crime investigation and intelligence activities, Decree 1704 of 2012 allows the Attorney General to ask telecommunications service providers personal data about a subscriber as well as real time geographic location of its device. Intelligence Law (Law 1621 of 2013) allows intelligence agencies to ask for "subscriber's communication history, technical identification data as well as cell location in which devices can be found and any other information that may contribute to its location" (Article 44).

Although vaguely defined, the data being referenced on those provisions must be kept by the telecommunication providers for 5 years[4].

Digital Citizen Services

From 2010, the Colombia Government has been pushing an agenda focused on ICTs and the development of a digital economy. In this context, a plan to create a personal "Citizen Folder" was presented in 2014. The idea behind the project was to offer a tool to easily

---

[2] https://wikileaks.org/hackingteam/emails/?q=DEA+colombia&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult

[3] https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

[4] Castañeda, J.D. "Is Data Retention Legitimate in Colombia?" Fundación Karisma. Available at: https://karisma.org.co/descargar/is-data-retention-legitimate-in-colombia/

store and share information with governmental agencies. From that moment on, the project was expanded and, by 2017, was approved through Decree 1413.

Digital Citizen Services include (1) electronic and (2) biometric authentication; (3) information interoperability between state agencies, (4) citizen folder and (5) electronic national ID card. This last element was never included on the public drafts that were publicly discussed. This infraestructural change is going to operate under a model in which any private party that complies with some requirements can offer any of those services. The requirements to offer those services are set by a governmental agency created to regulate these services.

This model poses great risk for personal data and the right to privacy since sensible personal data given to the State, in order to allow it to fulfill its constitutional mission, is going to be stored and processed by private parties under conditions determined outside parliamentary process. Given the level of ambiguity of this program, constitutional and legal barriers to access and process personal data might be bypassed.

Electronic Clinical and Labour Records

Following the approval of the Digital Citizen Services decree, the Ministry of ICTs presented a draft document in which electronic clinical records are incorporated and labour records are created and then also incorporated to the Digital Citizen Services model. Given that there are no agreed standards for the processing of medical data in Colombia and the lack of public participation on the development of this proposal, clinical and labor data might be at risk.

Data Exploitation Policy

Digital Citizen Services are in conflict with a proposal by the National Planning Department (NPD) regarding use of data by the State. Since 2015, NPD is seeking to publish policy guidelines in order to allow the State to exact “social and economical value” out of data the State posses. This data exploitation policy, under the draft version presented to the public, does not take into account issues regarding the exploitation of personal data and the pressures that monetization of government data might imply for the future of the Colombian’s right to privacy.

Conflicting policies might also endanger the legal context in which responsibilities may be diluted, rendering people’s rights useless or formally unprotectable.

5. Growing reliance on data-driven technology and biometric data:

Biometric Migration System (BIOMIG)

At the end f 2017, the Migration Control Authority[5] started using the BIOMIG system. This is a system of automatic identification that uses iris biometric data to identify Colombians over 12 years when entering the country through El Dorado International Airport. The system has 10 terminals and enrolling is voluntary.[6]

Gemalto, a Dutch company, is the private party in charge of developing the software to use the EF-45 terminals of biometric scanning made by CMI Tech. This company is also in charge of the biometric passport[7]. it has also the authentication system to access financial services of the Savings National Fund[8]. The same company works on biometric authentication of mobile financial services for banks.[9]

According to the Director of Migración Colombia, the terminal connects automatically with different national and international databases to verify if the person has a legal issue that prevents him or her to enter the country or if there is a warrant.[10]

[5]http://migracioncolombia.gov.co/index.php/es/prensa/comunicados/comunicados-2018/febrero-2018/6539-en-menos-de-25-segundos-y-con-solo-una-mirada-los-colombianos-podran-ingresar-al-pais-migracion-colombia
[6]http://es.presidencia.gov.co/noticia/180228-Migracion-Colombia-empezo-a-usar-sistema-de-inmigracion-de-colombianos-por-medio-de-reconocimiento-del-iris
[7] https://www.gemalto.com/press/pages/colombia-selects-gemalto-s-secure-epassport-solution.aspx
[8]https://www.symbolic.it/docs/Gemalto-SafeNet-Authentication-Service-Case-Study/Colombia_secures_citizens_access_to_financial_services_with_gemalto_strong_authentication.pdf
[9] https://www.gemalto.com/press/pages/news_266.aspx
[10]https://noticias.caracoltv.com/colombia/con-solo-una-mirada-colombianos-podran-ingresar-en-segundos-al-pais