Fundación Karisma
www.karisma.org.co

Mr. David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
Palais des Nations
CH-1211 Geneva 10
Switzerland

November 1, 2016

Subject: Study on Telecommunications and Internet Access Sector

Hereby, Fundación Karisma from Colombia presents its contribution on the study on freedom of expression in the telecommunications and Internet access sector, currently conducted by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

Introduction

Fundación 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, 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.

State Regulation: Data Retention for Criminal Investigation and Intelligence

In Colombia a provision that allows access to telecommunications and Internet services and networks is found on Decree 1704 (2012) by which technological infrastructure must be provided in order to guarantee "points of connection and access to communications traffic capture" to criminal investigation authorities acting under Articles 15 and 235 of the

Constitution that allows legal interception with judicial oversight and for criminal investigation purposes.

The same Decree allows criminal investigation authorities access to (1) subscribers' information "such as identity, billing address and connection type" and (2) geolocalization information "such as sectors, geographic coordinates and power" for the purpose of communications interception.

For intelligence purposes, Law 1621 (2012) requires telcos to hand over the "history of communications of their telephony subscribers, the technical identification data of the subscribers subject to the [intelligence] operation, as well as the cell location in which devices are located and any other information that may help with its localization"[1]. As explained in the following section (State Regulation: IMEI registry) specific metadata required from the operators may complete the meaning of the aforementioned "history of communications".

State Regulation: IMEI registry

Since 2011, the Colombian Government and the Telecommunications Regulator have been creating and developing an IMEI registry, allegedly to deter cellphone theft.[2] As a result, every device that works on mobile networks in Colombia, amounting to 52M according to the most accurate estimates, should be associated with an individual. This association is made through a "positive database" in which the IMEI of every device legally sold or imported is registered by the mobile telecommunications network operator ("operator") that activates the subscription including in the same registry, the name, ID number, address, and telephone number of the subscriber. Conversely, each telecom also operates a "negative database" in which irregular or reported as stolen or lost IMEI are registered.[3] For each registry, the operator must verify the subscriber's identity against the National Registry, financial risk databases or their own information. A third party collects the positive and negative databases of each operator and synchronizes them so as to avoid a reported device in one operator's network to work in a different one.

[1] A full analysis of the compliance with human rights standards of the data retention regime for criminal investigation and intelligence is available at https://karisma.org.co/is-data-retention-legitimate-in-colombia/

[2] The main legal document in which this system is established is Resolution 3128 of 2011 by the Telecommunications Regulator (Comisión de Regulación de Comunicaciones - CRC), available with following modifications at: https://www.crcom.gov.co/recursos_user/Normatividad/Normas_Actualizadas/Res_3128_11_Act_4986_16.pdf

[3] Besides stolen or lost devices' IMEI, the negative database includes IMEI without the proper format, without certificate of conformity or duplicated.

Article 9 of Resolution 3128 (2011) grants almost unfettered access by to authorities to this information. Specifically, it provides that administrative authorities "such as" Ministry of ICT (and others), "as well as" police and judicial authorities may query the updated information of the negative and positive databases "entry by entry." There is no oversight mechanism, nor requirement for these authorities to motivate the reasons for accessing the database, or any registry or logging of such queries.

Additionally, in order to detect irregular IMEI, especially duplicated IMEI, the regulation orders operators to collect and analyze voice Call Data Records (data CDRs are to be collected since 2017) and provide geographic coordinates of their cell phone towers to a third party. Specifically, the following information –metadata– should be analyzed by the operator:

1. IMSI, which comprises: MCC (mobile country code), MNC (mobile network code) and MSIN (mobile subscription identification number).
2. IMEI
3. Date and time of beginning of the event
4. Type of event: voice call or data session
5. MSC (Mobile Station Classmark): in case the operator should check the coherence of the information provided by the device.

The regulator and government, by setting this system, overlooked the protection of communications ordered by Articles 15 and 235 of the Constitution –judicial order in the context of a criminal investigation. When these concerns were raised during the regulatory process, the regulator asserted that the system is considered to be in compliance with Data Protection Law and thus, they argue, there is no bypass of privacy constitutional protections of any kind.

There are various scenarios when this system may come into play, deepening the risks to privacy. The customary (and sometimes arbitrary) police street search includes checking cellphone's IMEI. This search allegedly aims to catch blacklisted devices but the system has the capability to identify the user, its cellphone number and address in the database. Other scenarios may include the use of IMSI catchers to extract information in public demonstrations or surroundings of political or social organizations, for example, and the request of cell phone tower information that may be correlated with the cellphone registry. Also, intelligence services can access the information produced by the operators, specially the CDRs, thus giving meaning to the obscure provision of the Intelligence Law (Law 1621/2013) that required operators to hand over "history of communications" of its

customers (Article 44). Intelligence organisms lack proper control and the only mechanism of oversight, which is in charge of the Congress, is currently inoperative.

The system described does not put in place any measure remediate undue restrictions on access to operators networks, or undue access to subscribers' data.

Intermediaries role in the "Notice and Takedown" procedures

In March 2016 the hashtag #NoMasCensuraWinSports trended on Twitter in Colombia. It gathered together expressions of discontent shared by Colombian soccer fans on social media following the removal of their contents and, in some cases, the complete deletion of their accounts. However, this was only the gateway to the discovery of a much broader problem faced by other types of users besides football fans, such as musicians, designers, and cultural promoters who use social media to share content. Important cases similar to the ones described but regarding the political discussion had been documented also in countries such as Ecuador where parodies or critical discourse against the president has been taken down from the Internet when the government claims copyright ownership on the content that is been used such as news programs pieces or pictures.

Since 1998 internet intermediaries that are locate in the United States of America and has to do with copyright protected works (hosting, distributing searching, etc), must implement a mechanism known as "notice and takedown" that is described in the Digital Millennium Copyright Act (DMCA). The mechanism has been strongly criticized by civil society since it is a threat to freedom of expression in the digital world. It seeks to prevent digital piracy by imposing the intermediaries the obligation of taking down content when rightholders claim that there has been an infringement to their copyright. Once the content is no longer available on the Internet, the alleged infractors (users) are notified of the situation and can present a "counter-notice" explaining that they were not acting in bad faith, they can claim that their use was a "fair use" and request for the content to be uploaded again. If users fall into this conduct repeatedly their accounts can be cancelled.

In order to analyze the relationship between these types of cases and global discussions on intermediaries liability and the right to freedom of expression, Karisma undertook a research project based on the following hypothesis: the DMCA notice and takedown mechanism encourages intermediaries to intervene in the defense of the intellectual property rights of right holders in a manner that goes disproportionately against users, given their capacity to inform and be informed in the new digital environment. This effect is magnified by the mechanisms that content platforms such as YouTube, Twitter, Facebook,

Instagram, and others have implemented to comply with these legal requirements. The effect constitutes a major barrier against free expression and access to information that is worst for people in countries other than the United States. We believe that intermediaries should review the way in which they implement notice and takedown, and they should do so with a human rights perspective.

In our research, which is ongoing, we have identified at the following issues among others:

- Lack of transparency: (1) in their Terms and Conditions of Service, most platforms have no public information about the notice and takedown system and to that extent many users only become aware of the existence of such a system when they receive a notice themselves, and have no complementary information available to explain to them how it works, or that makes it clear that a counter-notice can be used to see whether the removal overlooked fair use; (2) once the notification process has begun, the platforms do not fully comply with DMCA stipulations regarding the obligation to send the user the claim that the holder has made on the content. This hinders access to information that is key if users are to send a counter-notice that includes all the points for which they were reported; and (3) it is unclear after how many notifications can an account be deleted. There is no information about this on the platforms, and yet account cancellations do occur.
- Notice and takedown mechanism implemented by platforms in compliance with the DMCA do not consider local contexts in which they operate and therefore do not guarantee the adequate defense of those people who can be affected by them. If users decide to continue the process -- i.e. sends the counter-notice -- and the claimant initiates legal action, defendants must accept the jurisdiction of US courts. This is a barrier that produces a chilling effect, that is, it causes enough intimidation to deter people from defending their rights to express themselves freely due to the threat of legal penalties.
- The main platforms are domiciled in the United States, and therefore the language in which they handle their communication is mainly English. Nevertheless, their global reach affects latitudes that are not necessarily native English speakers. In notice and takedown mechanism against users in Latin America, many of the notices come in English, which creates barriers for defense, where a legal message in a foreign language ends up causing the so-called chilling effect.

- There is little information on the response to a counter-notice: According to the DMCA, after the ISP receives a counter-notice by the person whose content was blocked or removed, they must send it to whomever reported the content. From

that moment, the intermediary has between 10 to 15 days to report whether the applicant brought an action before the court; if not, the platform must repost the blocked content or reinstate the account that was closed. From our analysis so far, seldom does a counter-notice have the desired effect, and rarely do people receive information about the reasons behind content being reposted or accounts reinstated.

We expect the result of this research to be published during 2016 and thus to be able to send more complete information in a few months. The research will show the Colombian case but since it is a standard procedure it could affect other countries too.

Net neutrality and plans offered by ISPs

Colombia established a net neutrality rule in the Law 1450 (2011) article 56. Afterwards the Regulatory Decree 3502 of 2011 amplified and detailed the neutrality rule. The regulation adopted principles and criteria to establish when a discrimination among contents, applications and services is considered to be arbitrary, and therefore against net neutrality. Those principles are: Free choice of the customer, nondiscrimination based on the property or the origin of the contents, transparency, and information. It is also included the criteria of illegal content.

Regarding the principle of nondiscrimination, it was clarified by the law and the decree that the ISPs have the ability to make offers to the needs of market segments or its users according to their use and consumption profiles. Therefore, the differential treatment of contents, applications and services according with specific use or consumption profiles is not regarded as discriminatory in itself. However this offers must comply with the aforementioned principles and criteria.

This ability enables ISPs to do all kinds of offers. It is feasible to restrict access to services, content and applications according to the type or nature of them, but not based on the supplier. Determine whether these distinctions are arbitrary or not depends on a case-by-case basis evaluation made by the regulator to determine whether or not the offer complies with the above principles.

Fundación Karisma is currently researching the Colombian net neutrality rule and how it compares with what has been said at the international debate, specially by academia and civil society organizations. During the preliminary stage of our research, we have identified difficulties applying the principle of freedom of choice for users. This principle is one of the bases of net neutrality highlighted both by doctrine and by national regulations. Therefore,

the regulator evaluates the degree of freedom of choice for users as criteria for determining a level of infringement to net neutrality. It is problematic that the principle is understood as the freedom to choose among plans offered and not between Content services or specific applications.

This is problematic for two reasons: (1) zero rating offers that have complied with the principle of free choice, do not give the user the freedom to choose the specific application they wanted in zero rating. On the contrary, the applications contents and services were predetermined by the ISP. (2) The most affordable or free deals offered by the government or ISP for digital inclusion, have a predetermined list of contents, application and services. Again, users are not free to choose and the services they will use are imposed. In this case, the absence of freedom to choose should be founded in technical requirements.

Sincerely,

Carolina Botero Cabrera
Director

Amalia Toledo Hernández
Project Coordinator

María Juliana Soto Narváez
Researcher

Juan Diego Castañeda Gómez
Researcher

Laura Daniela González Guerrero
Researcher