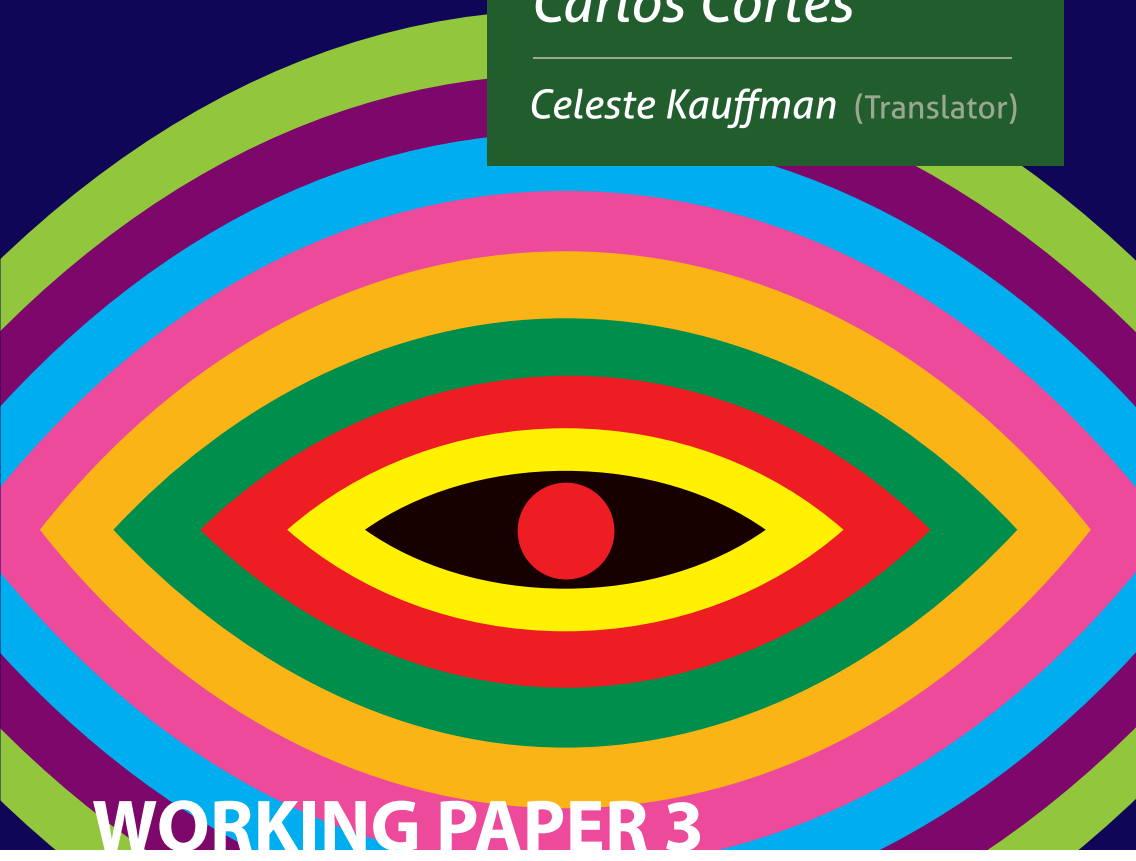
Communications Surveillance in Colombia

The Chasm between Technological Capacity and the Legal Framework

Carlos Cortés

Celeste Kauffman (Translator)



WORKING PAPER 3

Dejusticia
Law · Justice · Society

WORKING PAPER 3

Communications Surveillance in Colombia:
The Chasm between Technological Capacity and the Legal Framework

Carlos Cortés
Celeste Kauffman (Translator)

Carlos Cortés obtained his law degree from the University of los Andes (Colombia). He later graduated with a Masters degree Media Governance from the London School of Economics.

Celeste Kauffman is a researcher at the Center for the Study of Law, Justice and Society (Dejusticia). She obtained her law degree from the University of California, Berkeley, and her B.A. in Sociology, Spanish, and Women's Studies from Aquinas College.

Dejusticia
derecho · justicia · sociedad

Working Paper 3
COMMUNICATIONS SURVEILLANCE IN COLOMBIA:
The Chasm between Technological Capacity and the Legal Framework

This project was funded by Privacy International
and the International Development Research Centre (IDRC)

ISBN: 978-958-58464-7-0 Printed Edition
978-958-58464-8-7 Digital Edition

Center for the Study of Law, Justice and Society (Dejusticia)
Carrera 24 Nº 34-61, Bogotá, D.C.
Telephone: (57 1) 608 3605
E-mail: info@dejusticia.org
http://www.dejusticia.org

Translation: Celeste Kauffman
Copy Editing: Morgan Stoffregen
Layout: Marta Rojas
Cover: Alejandro Ospina
Printed By: Ediciones Antropos

Bogotá, January 2015

Contents

Special thanks to Vivian Newman, for her
advise in structuring this document;
to Dejusticia's researchers, for the comments
to the first draft, and to Juan Diego Castañeda,
for his support in the investigation phase.

Introduction

Last year, media outlets revealed that the National Police of Colombia would operationalize the Single Platform for Monitoring and Analysis (Plataforma Única de Monitoreo y Análisis, or PUMA), through which it would be able to intercept "what is spoken, written or sent from e-mails, Facebook, Twitter, Line, Viber, Skype, and, in short, any type of communication undertaken via the internet."[1] More recently, last February, *Semana* magazine revealed that the military was reviewing e-mails and chats of those involved in the peace talks in Havana, Cuba.[2]

In both cases, the government put its spin on the news. In the first case, the government presented PUMA as nothing more than the replacement of an older system, and stressed that it would be subject to legal controls.[3] In the second, the Colombian president quickly announced the formation of a commission to develop the country's policy on cybersecurity and cyberdefense.[4]

---

1 Policía podrá interceptar Facebook, Twitter y Skype en Colombia [Police may intercept Facebook, Twitter, and Skype in Colombia]. El Tiempo, June 22, 2013. Available at: http://www.eltiempo.com/justicia/ARTICULO-WEB-NEW_NOTA_INTERIOR-12890198.html (visited April 5, 2014) (author's translation).

2 Cf. Chuzadas: así fue la historia. [Wiretapping: Here is the story] Revista Semana, February 8, 2014. Available at: http://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3 (visited April 5, 2014).

3 La polémica que se desató por PUMA. [The controversy unleashed by PUMA] Revista Semana, June 29, 2013. Available at: http://www.semana.com/nacion/articulo/la-polemica-desato-puma/349109-3 (visited April 5, 2014).

4 Así construye Colombia su política de ciberseguridad y ciberdefensa. [How Colombia built its cybersecurity and cyberdefense policy] Enter.co, March 31, 2014. Available at: http://www.enter.co/chips-bits/seguridad/ciberdefensa-colombia-politica/ (visited April 5, 2014).

Nonetheless, the underlying issues remain unsolved. What is, in the end, the technical capacity of PUMA? Is it possible to review anyone's e-mails? Can the military access someone's chat history? Is intercepting a phone call the same thing as intercepting internet traffic?

Although new scandals regarding state intelligence emerge periodically in Colombia, the state never clarifies how intelligence works in practice or what controls exist for its exercise. Meanwhile, as time moves on, intelligence schemes grow more sophisticated along with our cell phones and computers.

An analog rotary-dial telephone is as obsolete as "crocodile cables" used to intercept calls. Nonetheless, as the market facilitates the process of obsolescence and the incorporation of new massive technologies, it tells us little about the devices that are simultaneously developed to monitor individuals.

Technological changes tend to alter long-established assumptions regarding the reach of specific rights. Privacy is arguably the right that faces the most challenges in the digital environment. Yet regulatory and jurisprudential lacunae persist in terms of how technology affects the exercise of fundamental rights.

The cases of PUMA and the military's spying on peace negotiators occurred soon after Colombia's adoption of its new Intelligence Law, which, in theory, corrects previous irregularities and aligns with modern surveillance. But is this truly the case? Do we have a regulation that preserves national security without compromising citizens' privacy and freedom of expression, among other rights?

The goal of this book is to examine the Colombian legal and jurisprudential framework regarding communications surveillance in light of today's technologies. Phrased in the form of a hypothesis, the purpose is to demonstrate how intelligence-related laws and jurisprudence fail to ensure that potentially affected rights remain intact.

To test this hypothesis, I address several aspects of the country's Intelligence Law that I selected somewhat arbitrarily: the interception of communications, surveillance of the electromagnetic spectrum, and access to user data. This last point, which alone merits its own study, is developed as a complement to the first two.

The book is divided as follows: The first chapter explains, from a technical point of view, the technologies that we use to communicate and that are used to monitor us. The second chapter explores the normative framework for communications surveillance. The third offers a comparative look at communications interception. Finally, the fourth chapter synthesizes the findings of the first three chapters in an effort to offer several conclusions.

Technology:
A Means to Communicate and to Monitor

The interception and monitoring of communications is as old as the forms of communication themselves. With letters and the postal service came the revision of envelopes and packages; with the telegraph came those who read telegrams; with the telephone came pincers to intercept cables.[1] Whether directly or through third parties, governments have always maintained some expectation of control over the words exchanged by their citizens.

Cell phones, the internet, and digital technology in general are no exception. Thus, just as today's communications are mobile, global, and instantaneous, the surveillance systems that underlie them operate from anywhere and in real time. With the same ease that two people talk, a third person observes or listens.

In this first chapter, I will explain the technical backdrop of the analog telephone, the internet, and the cell phone. From there, I will describe the technology used to intercept and monitor modern communications. As we shall see, there are diverse technological changes that determine and also require us to reconfigure monitoring schemes.

From the rotary phone to WhatsApp

Circuit switching and packet switching

The traditional telephone network was developed in the image and likeness of the railway network.[2] In fact, in many parts of the world, telegraph

1 Cf. Hosein, G. & Wilson, C. Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques. Ohio State Law Journal, Vol. 74:6, 2013 p. 1071-1104.

2 Cf. Landau, S. Surveillance or Security?: The Risks Posed by New Wiretap-

cables—the ancestor of the telephone—were installed alongside railroad tracks, and the offices of these services were housed in train stations. Over time, this communication network evolved in a decentralized but hierarchical manner, following patterns of cities and populations: a group of inhabitants connected to a telephone center, and a series of centers connected among themselves.

The first calls were made through an operator (generally a woman) who was responsible for connecting the ends of each network through manual switches. The telephone number indicated the city, the telephone center, and the destination number. With the arrival of automatic telephone switching, invented at the end of the nineteenth century by Almon Strowger, a North American, the process was made easier and networks began to expand.

The public telephone network assigns an exclusive channel for communication between two terminals. This method is known as circuit switching. In other words, when one person calls another from his home, the line can transmit only this conversation. Voice signals are transmitted as electronic pulses that make use of all the cable's capacity. Even if there is silence, the channel must be available for this communication.[3]

As the telephone network began to connect through providers, cities, and countries, it began to experience redundancies: there were several possible paths to get from point A to point B. Under these conditions, it was possible to establish various independent routes between distinct ends of the network. This was the general idea of the internet.[4]

The internet is nothing more than a hierarchical network of computers. Computer A is connected to a router (the blinking apparatus next to the computer); the router is connected to the service provider (Telmex, for example); the service provider is connected to a larger server; and this larger server is connected to a central server, known as a backbone. The route is the same from the backbone to computer B, but it is possible for the service providers of A and B to be connected between themselves, which means that the connection between A and B need not necessarily pass through the highest point of the network. In other words, an e-mail from pablo@telmex.com.co to sandra@etb.com.co may go simply from Pablo's computer to Telmex, from Telmex to ETB, and from ETB to Sandra's computer.

To take advantage of the network's capacity and to establish simultaneous connections, the internet utilizes a method different from circuit switching. This method, known as packet switching, divides data into packets at its point of origin and transports these packets, in a different order and through different routes, to their destination, where they are put together again and acquire their original meaning. The entire process follows a protocol of connection and transportation known as TCP/IP.

Packet switching is complemented by a principle of stratification, or of layers, which is known as the Open Systems Interconnection model. For the purposes of this book, it is enough to understand that each data packet has a series of layers: the most superficial layers contain the information needed to transport the packet and put it back together at its destination, and the deeper ones contain the data being transmitted. In this system, network routers are tasked with carrying the packets to their destination, which is why they need to "see" only the most superficial layers (as though they had to see only the address written on an envelope). The final terminals (for example, personal computers) take care of the rest. This is why the internet is known as a "dumb network," with intelligence only at its ends—and it is this design that supports the concept of internet neutrality.[5]

Let me illustrate this process with an example: when Andres sends an e-mail to Maria, Andres's computer divides the data in packets and sends them via the network. These packets travel through the network, directed by routers, in any order and through various routes. If we were to "observe" an individual packet during its journey, we would not see an intelligible conversation or message, as is the case with analog telephones. Rather, we would see only a portion of the data. When the data arrives at

ping Technologies. The MIT Press, 2010.

3 Cf. Farahmand, F. & Zhang, Q. Circuit Switching. In: The Handbook of Computer Networks. Volume II, 2007.

4 Cf. Wu, Tim. The Master Switch: The Rise and Fall of Information Empires. Random House, 2010.

5 For a more detailed explanation of the architecture of the internet, see Cortés, C. 'La neutralidad de la red: la tensión entre la no discriminación y la gestión' [Net neutrality: tension between non-discrimination and management], and 'Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en Internet?'[Monitoring the net: what does monitoring and content detection mean on the Internet?]. In: Internet y derechos humanos. Aportes para la discusión en América Latina [Internet and Human Rights: contributions to the debate in Latin America]. CELE, Palermo University, 2014.

its destination, Maria's computer puts the packets back together so that the e-mail appears as Andres wrote it. Thanks to the information contained in each packet, Maria's computer knows what order the packets should go in, as well as what application is capable of "reading" them.

Radio spectrum and mobile services

Cell phone and mobile services work in a different way. Rather than transporting data through cables, these services use the electromagnetic spectrum, which is the space made up of all the different sets of electromagnetic waves. The radio spectrum, in particular, refers to the band suitable for telecommunications services within the electromagnetic spectrum.[6]

Electromagnetic waves, like the ocean's waves, undulate and transmit energy—but unlike ocean waves, they "travel" through the air at the speed of light. The undulating character of the wave is the product of vibrations of the particles that it carries, which have magnetic and electric properties. If the amount of energy is low, the distance between two successive crests in the wave is large, and therefore we say that it has a low frequency (radio waves, for example, have this characteristic). By contrast, if the amount of energy is greater, the distance between each crest is very short and we say that the wave frequency is high (as is the case with X-rays or gamma rays). As the wave gets larger, its penetration is greater.

To offer mobile services, the government assigns network service providers one or more frequencies of the spectrum. These frequencies are the "highway" on which voice and data waves are transmitted. In light of the limited character of this portion of the spectrum, as well as its infinite capacity for reuse, these network service providers use transmission-receptor stations (or base stations) to carry data from one location to another. These stations are stationary and look like antennas.

When we make a call or send a text message from our cell phone, the strongest base station in the area—the one with the best signal—receives the data from our phone and transmits it to the strongest base station near the receiver. The latter, in turn, transmits the data to its recipient.[7] Each base station covers a limited area. Suppose that a station located on 100th Street in Bogota covers 90th Street to 100th Street (streets run east to west) and 1st Avenue to 25th Avenue (avenues run south to north). Beyond this circumference, the signal will be lost (the call will drop) or there will be interference.

To resolve this problem, network service providers install various stations and divide an area into many small regions, known as cells, which makes it possible to use the spectrum more efficiently, guarantee service, and satisfy a higher demand. The quantity of cells determines, along with other characteristics, the amount and conditions of data that may be transmitted. Thus, a city requires a higher-density network than do rural areas, as well as greater infrastructure.

The cell phone is always within the provider's radar. Each time we turn on our phone, or as we move with it, the strongest base station connects with the device to determine its identity and legitimacy within the system. This authentication is achieved through the International Mobile Station Equipment Identity (IMEI), a fifteen-digit serial number that identifies the device and associates it with a subscriber and a determined plan. (This also prevents, in theory, stolen cell phones from accessing the network).

In other words, for our cell phone to work, the service provider needs to know, with some level of precision, the zone in which we are currently located. Triangulating the data from various stations, a network service provider in an urban zone—which, as mentioned above, has an infrastructure closer to the user than it does in a rural zone—can determine our location within a fifty-meter radius.[8]

Data within data

The permanent location of our cell phone—which is generally also *our* location—is stored in the service provider's history, along with data regarding calls made and received, the length of those calls, and (when the user has internet service) web pages visited and applications used.

Smart phones have additional technology that permits the determination of the user's location. On one hand, these devices can connect to wireless networks (Wi-Fi), with which they share information in order to access the internet. On the other, they have Global Positioning Sys-

6 This chapter is based largely on Poole, I. Cellular Communications Explained. From Basics to 3G. Newnes, 2006.

7 Voice and data transmission in mobile services follows a method similar to packet switching in landline internet. That is, it is not the voice as such that "travels" but rather a series of packets with portions of data that are reorganized at their destination.

8 Cf. Pell, S. & Soghoian, C. Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact. Berkeley Technology Law Journal, Vol. 27, p. 117, 2012.

tems (GPS), which serve as the basis for location-based services, such as "Maps," "Find My Friends," and "Foursquare"—applications that geographically reference the user or that, based on the user's location, offer a particular service.

This data does not in itself contain the conversation, message, or object of communication; rather, it simply contains some information regarding its content. This is what is known as metadata: data that describes other data.[9] A telephone number or the duration of a telephone call does not tell us what the call was about, nor does the e-mail address or the number of messages sent tell us what was contained in those messages. Nonetheless, they provide valuable information about the purpose of the communication. This is even more certain if the data can be indexed and analyzed.

In addition to these digital trails left behind by our communications, the applications and services that we access from our cell phones and computers (whether from landline internet or wireless internet) are true personal files: Gmail contains all of our e-mails from the past several years; Twitter has dozens of direct messages; Flickr houses photos and videos; and WhatsApp records both trivial and transcendental conversations. These are no longer metadata but rather data saved in the servers of those who administer the applications or social networks that we use.

Modern forms of surveillance

The interception of a call made through a switched telephone network is relatively simple: at any point in the communication—whether in one of the telephones, a point along the cable, connection boxes, the phone center, or posts—a device is placed that sends signals allowing a third party to listen to or record the conversation.[10]

It seems clear that this procedure would not work for intercepting a cell phone conversation or an e-mail exchange. Nonetheless, that there are distinct ways of monitoring modern communications does mean that there are clear boundaries between the ways of doing it on the applicable platforms. Instead, surveillance follows a paradigm of access: How do we access a communication? Where do we enter? How do we obtain what we need? Taking place today is the expansion of surveillance technologies whose principal characteristic is ubiquity and the capacity to integrate into the modern communication architecture.[11]

Gus Hosein and Caroline Wilson identify three types of communications surveillance that are used around the world: (i) the targeted use of offensive technologies; (ii) targeted and semi-targeted technologies for cell phone surveillance; and (iii) massive internet surveillance.[12] These categories offer a methodological orientation.

The targeted use of offensive technologies

The targeted use of offensive technologies permits agents to circumvent the need to physically seize a device for inspection. Without knowing the owner of the equipment and from a distance, agents use the back doors of operating systems or particular programs—or they create them with malware or Trojans. This is why such technology is referred to as offensive.

Programmers tend to include back doors in systems and applications in order to enter them when they have errors or are damaged, or when there is no access through the front door (which requires a user name and password). Thus, back doors are a privilege of the creator or administrator of the applications, sometimes legally required precisely in order to facilitate intelligence work. Back doors are not bad in and of themselves, but they can exist and operate without the user's knowledge. Or worse—they can be created by installing malware or Trojans in the machine.

To open or create a back door, the agent must acquire control of the machine that he wishes to monitor. If the agent has physical contact with the computer, he simply installs a Trojan using a USB device or CD. If the agent is creating a back door remotely, he must trick the user into installing malware by making the user think that it is something else.

In April of last year, the Mozilla Foundation announced that the German company Gamma International had created a false Firefox browser in order to install Trojans for surveillance purposes. Thus, users downloaded certain files thinking that they were installing the latest version of Firefox when, in reality, they were activating a back door on their computers. Be-

9 Cf. Mayer-Schönberger, V. & Cukier, K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, 2013.

10 Cf. Op. Cit. Landau, S.

11 Cf. Citizen Lab. For Their Eyes Only. The Commercialization of Digital Spying. Marquis, M. et al. University of Toronto, May 2013.

12 Op. Cit., Hosein, G. & Wilson, C.

yond whether the practice was legal, Mozilla claimed that the false browser was affecting the company's product and brand.[13]

The Citizen Lab at the University of Toronto has documented similar cases in the context of the Arab Spring. In Bahrain, for example, activists were the objects of attack by Trojans attached to e-mails. The activists received e-mails ostensibly from a well-known reporter who was sharing pictures of arrested activists. When the activists downloaded these pictures, they also installed malware onto their computers. The reporter's e-mail account, it seems, was false.[14]

Once a back door is open and a Trojan is installed, the agent acquires control over the computer, assuming that the computer is connected to the internet. It is as if the agent has entered our home: he can harvest data, download files, extract user names and passwords, turn on the computer's camera, control the keyboard, and monitor Skype, among other things. If the Trojan is installed in a cell phone, the agent can even activate a "silent call" whereby the computer becomes a microphone.

Various companies develop and commercialize these types of offensive technologies. The false update of Mozilla, in particular, forms part of a product called FinFisher, which is used in at least twenty-five countries (including Mexico). FinFisher advertises itself as a "remote surveillance solution" that collects information from the infected computer and sends it to a server.[15]

Targeted and semi-targeted technologies for cell phone surveillance

Targeted and semi-targeted technologies for cell phones allow third parties to actively monitor mobile communications. Depending on how the technologies are used—and as their name implies—they can be targeted to a specific object or be employed indiscriminately against all individuals with cell phones in a given area.

The most common device, known as an IMSI catcher (short for International Mobile Subscriber Identity), is one that simulates a cellular station. It is known on the market by the brand StingRay, manufactured by the North American company Harris Corporation. In September 2013, the most advanced version of the StingRay cost around US$135,000. This mobile device does not require a physical connection to the network in order to operate, and it fits easily into the trunk of a small car. The device is impossible for cell phone users to detect and is very difficult to discover even for cell phone service providers.[16]

StingRay functions by passing itself off as the cellular station with the best signal for the cell phone that is the object of monitoring (remember that cell phones are constantly connecting to the station that emits the best signal in the area) in order to identify the object's IMSI. The IMSI, as its name implies, is the identity of the device within the network; it is always associated with a phone number and, therefore, a subscriber.

As Hosein and Wilson explain, "By impersonating a base station, all mobile phones on that network in that area will connect to the monitoring device rather than the legitimate network. The device can therefore identify all phones within range. In a more advanced implementation, they can also enable direct access to communications content and metadata by routing calls through the base station."[17]

In other words, this device can identify one or several cell phones of individuals in a public or private place: for example, during a demonstration or a closed-door meeting. It is sufficient to cross the IMEI with telephone numbers and their account holders; the latter is information that network services providers are usually obligated to provide. In its most sophisticated mode, the StingRay can intervene in an individual transmission in order to obtain access to the data that passes through that transmission.

Another IMSI receptor available in the market is the Gossamer, a portable device the size of a 1980s cell phone, which, in addition to locating cell phones in a given zone through the IMEI, may block the target phone from making or receiving calls (this type of attack is known as a denial-of-service attack). In 2013, the Gossamer sold for around US$20,000.[18]

13 Cf. Protecting our brand from a global spyware provider. Mozilla. In: https://blog.mozilla.org/blog/2013/04/30/protecting-our-brand-from-a-global-spyware-provider/ (visited April 1, 2014).

14 Cf. Op. Cit. Citizen Lab.

15 Cf. 'You Only Click Twice: FinFisher's Global Proliferation'. Marquis-Boire, M. et al. The Citizen Lab, Munk School of Global Affairs, University of Toronto. Research Brief No. 15, March 2013.

16 Cf. Strobel, D. IMSI Catcher. Seminararbeit Ruhr-Universität Bochum, 2007.

17 Hosein, G. & Wilson, C., p. 1081.

18 Cf. Meet the machines that steal your phone's data. Arstechnica, available at: http://arstechnica.com/tech-policy/2013/09/meet-the-machines-

Massive network surveillance technologies

Massive network surveillance technologies are aimed at collecting large quantities of information for later analysis. The best example of this type of surveillance is that of the Prism scandal, uncovered in 2013 by the *Guardian* and other media outlets.

According to information revealed by ex-CIA contractor Edward Snowden, the National Security Agency of the United States had acquired access to the databases of Google, Facebook, Apple, and other internet service providers. Users' search histories, e-mails, files, and chats, among other things, had found their way into the hands of US intelligence officials.[19]

In general terms, there are two methods for accessing such information: by collaborating with the service provider or by surreptitiously opening a back door or observing traffic that passes through a given point on the network. These two options are not mutually exclusive. Media reports point to a combination of collaboration among intermediaries (Google, Facebook, Yahoo, etc.) and the monitoring of cables and network tubes.[20]

Under the first method, internet service providers and state agencies have a mechanism for sharing information. This may be either a permanent passing of information or, perhaps more likely, a back door created by the companies that allows agents to easily consult the information they need.

Under the second method, government agents use technology to monitor traffic at strategic points of the internet. As described above, the internet is a hierarchical network with local servers, points of connection, backbones, and underwater cables between countries. Depending on where the device is placed, there will be more or less data to analyze.

that-steal-your-phones-data/ (visited April 2, 2014).

19 Cf. 'NSA Prism program taps in to user data of Apple, Google and others'. The Guardian, June 7, 2013. Available at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (visited March 18, 2014).

20 Cf. 'US tech giants knew of NSA data collection, agency's top lawyer insists.' The Guardian. Available at: http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de (visited March 19, 2014).
See also 'The Creepy, Long-Standing Practice of Undersea Cable Tapping.' The Atlantic, June 16, 2013. Available at: http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/ (visited March 19, 2014).

Either way, this work is very complex due to the immeasurable amount of data that passes through the cable, and it requires equipment that can analyze traffic in search of data packets with information or key words.

One of the technologies used for this task is deep-packet inspection. As explained above, data travels through the internet in packets, which in turn are divided into layers; the outer layers include basic information that identifies the packet, while the deeper layers include the information being transmitted. Through a black box, which must be connected to some point along the network, traffic is analyzed, packets are selected, and the deeper layers are examined in order to identify certain contents.[21]

The outer layers of the packets contain relevant metadata, such as the recipient's e-mail address, the message subject, and the application being used. Thus, although the actual information being transmitted cannot be seen, these outer layers already provide useful information to copy, index, and analyze. And although there are technologies (encryption technologies) to code this data in such a way that only authorized parties have access to it, social networks and online services do not generally make use of these tools.

Some of the technologies referred to in this chapter are not designed exclusively to monitor the activity of internet users. They are also meant to monitor the system's functioning, improve quality of service, and prevent the use of malware. Therefore, they are available to service providers and network service providers, which makes their control even more difficult.

Communications Surveillance in Colombia

The Colombian legal regime differentiates between the interception of communications and surveillance of the electromagnetic spectrum. While the former is undertaken in concrete criminal investigations—via a criminal notice and in order to search for evidence to identify the authors of a crime—the latter forms part of the state's intelligence activities. It is undertaken not to pursue a specific person but to prevent illegal uses of the spectrum.[22]

21 For a detailed explanation of deep-packet inspection, see Cortés, C. El deseo oficial de vigilar la red. Monitorear y detectar contenidos en Internet [The Official Desire to Monitor the Net. Monitoring and Detecting Internet Contents]. In Op. Cit. Palermo University.

22 Cf. Constitutional Court, Decision T-708 of 2008, Presiding Magistrate Clara Inés Vargas, and C-540 of 2012, Presiding Magistrate Jorge Iván

In this chapter, I explain each of these concepts from the perspective of constitutional jurisprudence, the Criminal Code, and the Intelligence Law, the latter of which was recently passed by Congress and endorsed by the Constitutional Court. I also refer to the powers that authorities have—both in criminal investigations and in intelligence activities—to access user data held by service providers.

Criminal investigations

The International Covenant on Civil and Political Rights establishes that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." In order to put this guarantee into practice, it adds that everyone must have legal protection against such interferences.[23] In identical wording, the American Convention on Human Rights also recognizes the right to privacy.[24]

Both of these instruments form part of the "constitutional block." This means that human rights guarantees that have been endorsed by Colombia and incorporated into the country's normative framework have the same legal ranking as the Constitution. Article 15 of the Colombian Constitution, similar to the language provided by the International Covenant on Civil and Political Rights and the American Convention on Human Rights, guarantees the right to privacy in the following terms:

> All people have the right to personal privacy and that of their family, as well as to their good name, and the State must respect those and ensure that others respect them. Additionally, all people have the right to know, update and correct information that has been collected about them in databases and files of public and private entities.
>
> In the collection, treatment, and circulation of data, freedom and other rights consecrated in the Constitution shall be respected.
>
> Correspondence and other forms of private communication are inviolable. They may only be intercepted or searched with a warrant, in the cases and with the formalities that the law establishes.

In a complementary manner, article 28 of the Constitution relates to the right to privacy and establishes that "every person is free" and that a person's home may be searched only "in virtue of written warrant of the authorized legal authority, with all relevant formalities and for reasons previously defined by the law."

Private communications are thus inviolable, except in cases where a judge previously authorizes their interception in conformity with procedures established by law. It is only with this level of protection that arbitrariness and abuse of administrative authority may be avoided.[25]

With the arrival of the adversarial criminal justice system, an exception to such requirements was introduced. Article 250 of the Constitution was modified in order to grant the General Prosecutor authority to "carry out searches, seizures, and interceptions of communications. In such events, the presiding judge will ensure the legality of such actions within thirty-six (36) hours of the event."[26] Thus, this article grants the prosecutor authority to undertake interceptions without obtaining prior authorization, but with later legal control.[27] Later, Law 1453 of 2011 shortened the timeframe from thirty-six to twenty-four hours. Considering that it was a more protectionist standard, the Constitutional Court declared this adjustment constitutional.[28]

Under article 235 of the Criminal Proceedings Code, the prosecutor may order "the interception through tape recording or similar technology of communications that travel through any communications network in which there is information or interest regarding the purpose of the proceedings". This order is valid for six months with the possibility of an extension.

According to the Constitutional Court, the prosecutor requires this faculty in order to rapidly collect information that is about to disappear or be altered. However, according to the court, the interception, search, or seizure is valid without a warrant only if there is a legitimate risk that such information will disappear or be altered.[29]

Palacio Palacio.

23 International Covenant on Civil and Political Rights.

24 American Convention on Human Rights, articles 11(1)-(3).

25 Cf. Constitutional Court, decision C-179 of 1994, Presiding Magistrate Carlos Gaviria Díaz, and T-343 of 1993, Presiding Magistrate Fabio Morón Díaz.

26 Political Constitution of Colombia, article 250(2).

27 Law 1453, article 68.

28 Cf. Constitutional Court, decision C-131 of 2009, Presiding Magistrate Nilson Pinilla Pinilla.

29 Cf. Constitutional Court, decision C-336 of 2007, Presiding Magistrate

The presiding judge is charged with examining the prosecutor's actions and determining whether they respect citizens' fundamental rights. This control can have two results: If there was a violation of the object of the investigation's rights, the prosecutor's actions are considered illegitimate, and the evidence collected is often invalidated and considered impermissible in criminal proceedings. By contrast, if the judge determines that the prosecutor did not go beyond the limits of his power, the judge will approve the evidence.

Specifically, the prosecutor's actions must comply with the requirement of proportionality. In the words of the Constitutional Court, the trial judge must verify "whether the measure that affects the exercise of a fundamental right (i) is adequate to contribute to reaching a constitutionally legitimate goal; (ii) is necessary in that it is the least restrictive measure available to achieve the goal; and (iii) if the goal pursued by the rights affectation compensates the sacrifices that this affectation causes for rights holders and society."[30]

Decree 1704 of 2012, which regulates Criminal Code reform, defines legal communications interception without distinction as to the "origin of the technology." It simply affirms that such interception involves "a mechanism of public security that seeks to optimize the task of investigation of crimes carried out by authorized bodies and authorities, within the constitutional and legal framework."[31] For the judicial authority to carry it out, network service providers must guarantee "at all times the technological infrastructure necessary to provide connection points and access to the capture of communication traffic that passes through their networks."[32] Thus, providers must guarantee an infrastructure that allows government access or a back door in order to carry out an interception.

Interception without a warrant, save the prosecutor's exception discussed above, is a crime. Article 269C of the Criminal Code establishes that "he who without previously obtaining a warrant intercepts information at its point of origin, destination, or within information systems, or in electromagnetic emissions from an information system that transports them, will be subject to 36 to 72 months' imprisonment."[33]

Jaime Córdoba Triviño, and C-334 of 2010, Presiding Magistrate Juan Carlos Henao Pérez.

30 Constitutional Court, decision C-591 of 2005, Presiding Magistrate Clara Inés Vargas (unofficial translation).

31 Decree 1704 of 2012, article 1 (unofficial translation).

32 Id. article 2 (unofficial translation).

Intelligence activities

Monitoring the electromagnetic spectrum is part of the state's intelligence and counterintelligence activities. It is a task included within the state's goals of "defending national independence, maintaining territorial integrity and ensuring peaceful coexistence and validity of a just order,"[34] as well as within the police's and military's goals of defending national sovereignty, territorial integrity, and the constitutional order[35]

Article 2 of the Intelligence Law (Statutory Law 1621 of 2013) establishes that the tasks of intelligence and counterintelligence include the "collection, processing, analysis, and diffusion of information" to prevent and combat internal or external threats to the democratic, constitutional, or legal regime, or to national defense and security.

The police and military, through specialized offices, are authorized to carry out intelligence and counterintelligence activities. They can also perform such activities through the Financial Information and Analysis Unit, an entity dedicated to combating money laundering, and any other entity authorized by law. This means that the National Intelligence Bureau, created in 2011 to replace the Administrative Department of Security, also enjoys this power.[36]

According to article 17 of the Intelligence Law, "the interception of private landlines or cell phone calls, as well as private communications of data, must comply with the requirements established in article 15 of the Constitution and the Criminal Code, and may be carried out only within the framework of judicial proceedings." This means that they require the same

33 Unofficial translation.

34 Political Constitution, article 2.

35 Cf. Articles 217 and 218 of the Political Constitution. See also Constitutional Court, decisions C-913 of 2010, Presiding Magistrate Nilson Pinilla Pinilla; T-066 of 1998, Presiding Magistrate Eduardo Cifuentes Muñoz, and T-444 of 1992, Presiding Magistrate Alejandro Martínez Caballero.

36 Intelligence Law, article 3. Also, article 18(a) of Law 1444 of 2011 grants the Colombian president the extraordinary authority to create administrative departments. As a result, the National Intelligence Bureau (DNI, for its Spanish acronym) was created via Decree 4179 of 2011. The bureau functions as "a civil security organ, which develops strategic intelligence and counterintelligence activities" (article 1). For the effects of Law 1621 of 2013, the DNI is thus an organ that carries out intelligence and counterintelligence functions.

level of judicial control as general investigations. Surveillance of the spectrum, by contrast, "does not constitute interception of communications."

According to the Constitutional Court, surveillance of the spectrum consists of carrying out "preventative inspection measures"[37] and includes "a type of tracking of shadows, images, and sounds represented in electromagnetic radiation frequencies and radio electric waves."[38] Unlike interception, which involves targeted, individual action, surveillance involves the "incidental capture of communications revealed in situations that allow the avoidance of attacks and to control risks for the national defense and security of the Nation."[39]

According to the court's criteria, surveillance is a passive activity carried out under the reasonable suspicion that a crime is being prepared or committed. It must be carried out only "to obtain information that is strictly necessary regarding suspicious or fraudulent operations, during a determined lapse of time, without violating the right to privacy, and strengthening the corresponding confidentiality to protect the good name of individuals."[40] Additionally, surveillance must be proportionate, subject to legal proceedings, carried out under supervision and control, and provide complaint mechanisms for those affected.[41]

Nonetheless, the Intelligence Law does not provide a complaint mechanism for individuals affected by intelligence activities. Its control and supervisory mechanisms are established according to the following terms:

- The monitoring of the electromagnetic spectrum, as with any intelligence activity, must be authorized via an operations order or work mission, which may be issued by agency directors or the chiefs or deputy chiefs of particular units, sections, or local entities, as applicable.[42]

37 Constitutional Court, decision T-708 of 2008, Presiding Magistrate Clara Inés Vargas (unofficial translation).

38 Constitutional Court, decision C-540 of 2012, Presiding Magistrate Jorge Iván Palacio Palacio (unofficial translation).

39 Constitutional Court, decision C-540 of 2012, Presiding Magistrate Jorge Iván Palacio Palacio (unofficial translation).

40 Cf. Constitutional Court, decision T–708 of 2008, Presiding Magistrate Clara Inés Vargas.

41 Cf. Constitutional Court, decision C-540 of 2012, Presiding Magistrate Jorge Iván Palacio Palacio. See also Constitutional Court, decision 1037 of 2008, Presiding Magistrate Jaime Córdoba Triviño.

42 Article 14.

- Authorization via an operations order or work mission must take into account "their nature and possible impact, the type of objective, the level of risk for agents, and the possible limitation of fundamental rights."[43]
- Any information collected that does not fulfill the aforementioned goals must "be destroyed and may not be stored in intelligence and counterintelligence databases."[44]
- Failure to comply with duties or obligations by officials charged with intelligence activities constitutes poor conduct and may lead to civil, criminal, economic, or professional sanctions. Exemption of responsibility for obedience does not apply in cases of violations of human rights or international humanitarian law.[45]
- The Legal Commission on the Monitoring of Intelligence and Counterintelligence Activities is a congressional body whose objective is to politically control the use of resources and ensure respect for the Intelligence Law in intelligence activities.[46]
- On an annual basis, the relevant police or military inspector, or the person acting on his behalf (in the case of the Financial Information and Analysis Unit and the National Intelligence Bureau), must provide a confidential report to the Ministry of Defense, with a copy to the Legal Commission on the Monitoring of Intelligence and Counterintelligence Activities, regarding the observance of the principles and limits established in the Intelligence Law.[47]
- The final part of article 18 establishes that inspectors will have the support of "different bodies, who shall not reveal for any reason their sources and methods." However, when the Constitutional Court studied the constitutionality of this article, it noted that this reservation "does not prevent that only control and supervisory bodies can access [the information] in order to fulfill their duties. The condition of no revelation cannot be claimed before a judicial authority in an investigation."[48]

43 Article 14.

44 Article 17.

45 Article 15.

46 Article 20.

47 Article 18.

48 Constitutional Court, decision C-540 of 2012, Presiding Magistrate Jorge

- Officials of these bodies are required to report irregularities in the exercise of intelligence activities to the corresponding inspector or the director or chief of the intelligence body. The directors or chiefs, in turn, must report annually to the president regarding such irregularities.[49]

User data

As discussed above, user data held by network service providers is fundamental to modern surveillance. It is more than a mere complement or starting point for an investigation; indeed, on its own, it can be sufficient to monitor an individual's activities. Here it is also necessary to distinguish between criminal investigation activities and those limited to state intelligence and counterintelligence.

Decree 1704 of 2012 establishes an illustrative rather than exhaustive list of the type of subscriber information that 'network providers and telecommunication services' must make available.[50] According to article 4, they must provide the prosecutor or "other relevant authorities" subscriber data "such as identity, billing address, and type of connection. This information should be handed over immediately."[51]

Additionally, article 5 requires providers to furnish "specific information contained in their databases, such as sectors, geographic coordinates, and strength, among others, that help determine the geographical location of terminal equipment or devices participating in the communication. This information must be provided online or in real time in cases that so require it."

In 2007, the Constitutional Court determined that selective searches of the databases of public or private entities require a warrant.[52] For intelligence and counterintelligence activities, however, no such warrant is required. According to article 44 of the Intelligence Law, network service providers (referred to in the law as 'operators of telecommunications services' (network service providers) have the duty to collaborate.

Concretely, this means that at the request of a state intelligence agency during an authorized operation, the service provider must deliver "the communication history of the relevant subscriber telephones, technical identification data of the subscriber who is the target of the operation, as well as the location of the cells in which the terminals are located and any other information that will help determine their location." Service providers are required to store user information for five years.[53]

Communications Interception in Other Countries

Three fundamental points stand out after reviewing the Colombian normative framework on communications surveillance in intelligence activities: the distinction between surveillance and interception, the different requirements for carrying out these two activities, and the types of controls that apply to them.

In this chapter, I will undertake a brief comparative look at this issue. As we shall see, in the countries explored here, surveillance and interception form equal parts of the state's intelligence activities and are therefore subject to the same controls. The latter, additionally, tends to be subject to internal control mechanisms or special judicial supervision.

United Kingdom

Communications interception in the United Kingdom is regulated by the Regulation of Investigatory Powers Act (RIPA) of 2000. Before discussing the law, it is useful to briefly provide some context: in 1984, in *Malone v. The United Kingdom*, the European Court of Human Rights ruled that England and Wales had violated the European Convention on Human Rights by failing to adopt regulations regarding telephone interception, in contravention of article 8 of the convention, which protects privacy and family life.[54]

As a result of this decision, the UK Parliament issued the Interception of Communications Act in 1985. This time, the European Court of Human Rights found the new law insufficient, as it focused on commu-

Iván Palacio Palacio.

49 Article 18.

50 The decree opts for this name rather than that used by the Intelligence Law: "operators of telecommunications services."

51 In July 2013, the Council of State provisionally suspended the phrase "and other competent authorities" while it resolves a request of nullity filed against the decree.

52 Cf. Constitutional Court, decision C-336 of 2007, Presiding Magistrate Jaime Córdoba Triviño.

53 Intelligence Law, article 44, and Decree 1704 of 2012, article 4.

54 Cf. Oxford Pro Bono Public. Legal Opinion on Intercept Communication. The Justice Project, Oxford University, 2006.

nications sent by post or through public telecommunications systems, thus leaving private communications exempt from legal controls.[55] This ruling, together with the passage of the Human Rights Act in 1998, which incorporated all the rights contained in the European Convention on Human Rights, led to the adoption of RIPA, which proposes a broader legal framework regarding state surveillance powers.

RIPA thus regulates the state' undercover monitoring activities, such as the use of trackers and hidden cameras, as well as the interception of communications, from phone calls to e-mails. It applies to, among other bodies, the police, intelligence services (M15, M16, and GCHQ), and even local government agencies.[56] Communications interception is defined as any undercover action directed at acquiring the contents of messages or conversations transmitted via a network or distributed by a service.[57]

The first section of RIPA establishes that it is a criminal offense to intentionally intercept the communications of any person without lawful authority. Lawful authority is an order issued by the Secretary of State or a senior official in exceptional circumstance. The secretary must certify that the interception is undertaken in the interest of national security, in order to prevent or detect a serious crime, or to safeguard the United Kingdom's economic interests.[58]

Nevertheless, such an order is not required under the following circumstances:

- When both parties agree to the interception or are reasonably believed to have given their consent.
- When one of the parties has given his consent—for example, when one of the parties is the person recording the conversation, and the monitoring is targeted (this provision of RIPA refers to undercover surveillance that does not involve entering into a home or private space and is made while carrying out an operation or investigation).
- When the communication takes place in a private telecommunications network (a company, for example) and the person who controls the system (the boss or chief) has consented to the interception.
- When the communication is made from a prison or psychiatric hospital.
- For a request for communications interception to be approved, the secretary of state must ensure that the interception is necessary (i) for the interest of national security; (ii) to prevent or detect a crime; or (iii) to safeguard the economic well-being of the United Kingdom.

The Interception of Communications Commissioner's Office is responsible for the supervision of interception orders. The commissioner, who must occupy or have occupied a high position in the judiciary,[59] is responsible for reviewing interception orders but does not have the authority to review the process or the justification underlying each order.

The body that does have this power is the Investigatory Powers Tribunal, which processes complaints against public entities with respect to communications interceptions or other activities authorized under RIPA. Specifically, the tribunal can annul interception orders or order the destruction of any material resulting from the surveillance.[60] Nonetheless, RIPA decisions may not be appealed or questioned before any court. There are also no oral hearings, accusations, interrogations, or opportunities to question evidence. In the end, a person who has reason to believe that he has been the target of irregular interceptions cannot have any expectation of the tribunal resolving his case or providing him with information about it.[61]

Chile

The Chilean law regarding the state intelligence system recognizes that when there is a need to obtain certain information unavailable through "open sources," "special procedures to obtain information" may be employed to protect national security and "Chile and its people from threats of terrorism, organized crime, and drug-trafficking."[62]

55 Cf. European Court of Human Rights. Halford vs. United Kingdom, 1997.
56 Cf. Open Rights Group. 'Digital Surveillance'. Why the Snoopers' Charter is the wrong approach: A call for targeted and accountable investigatory powers.
57 Cf. JUSTICE. Freedom from Suspicion Surveillance Reform for a Digital Age. 2011.
58 RIPA, section 5(5).
59 RIPA, section 57(5).
60 RIPA, section 67(7).
61 Cf. Op. Cit. JUSTICE.
62 Law 19.974 of 2004, article 23.

The procedures authorized to access "closed sources" are the following:

a) intervention of telephone, information, and radio communications, and correspondence in any form;
b) intervention of information systems and networks;
c) listening to or electronic recording (including visual recording); and
d) intervention in any other technological system used to transmit, store, or process communications or information.[63]

The use of any of these procedures requires judicial authorization. The authorization must be requested by the director or chief of the relevant intelligence body, and will be granted only to detect, neutralize, or counteract actions of domestic or international terrorist groups or transnational criminal organizations, or the intelligence operations of other domestic or foreign groups.[64]

Chilean law also states that the authorization of such procedures "must include the specification of methods to be used, the identification of the person or persons against whom the measure will be used, and the timeframe for which it is decreed, which may not be longer than ninety days, extendable for one additional ninety-day period."[65]

Intelligence activities are subject to internal and external controls. Internal controls are exercised by the director or chief of each intelligence body, who is also the person directly responsible for compliance with the law. This control includes the use of human and technical resources, the rational use of funds, and respect for constitutional and legal guarantees in the development of intelligence operations.[66]

External control is exercised by the Office of the Comptroller General of the Republic and by the Senate. The former is responsible for ensuring the legality of the actions (known as a record of endorsement) of the National Intelligence Agency.[67] Through a special commission, the Senate is responsible for reviewing the activity reports of intelligence bodies in closed sessions.[68]

63 Id., article 24.
64 Id., articles 25 and 27.
65 Id., article 28.
66 Id., articles 33 and 34.
67 Id., article 36.
68 Id., article 37.

Although the norm also identifies courts as external control mechanisms, it does not specify their powers beyond indicating that they shall act within "their respective powers."[69] In any event, the duty to maintain the confidentiality of intelligence activities may not take precedence over requests made by courts, the Senate, or the Public Ministry, among others.[70]

Mexico

Article 16 of the Mexican Constitution provides that only the federal judicial authority, at the request of a competent federal authority or the public ministry of the relevant state, may authorize the interception of a private communication. In its request, the interested authority must specify the justification for the activity, its duration, and the type of investigation.

Mexico's National Security Law submits communications interventions for intelligence and counterintelligence purposes to a special standard of judicial control. Under article 34, "communications interventions refer to the taking, hearing, surveillance, monitoring, recording, or register, by an authorized body, of private communications of any type and by any method, apparatus, or technology."[71] Intervention thus includes both surveillance and interception activities.

Under this law, communications intervention may proceed only in the presence of threats to national security, including, among others, espionage, sabotage, terrorism, rebellion, and treason.[72] In such cases, authorities must follow an exceptional procedure to obtain authorization, which must be responded to within twenty-four hours of the request. The authorization must include a description of the intervention's facts (omitting details that put the operation at risk), justification, and timeframe.

In the resolution approving the measure, the judge must specify the type of activity to be carried out, the timeframe, and the authorization to install or remove equipment related to the operation.[73] Authorization is granted for a maximum of 180 days, with the possibility of an additional 180-day extension. Eventually, the judge may request periodic reports

69 Id., article 36.
70 Id., article 39.
71 National Security Law. Official Gazette of the Federation of January 31, 2005. Available at: http://mexico.justia.com/federales/leyes/ley-de-seguridad-nacional/ (visited April 3, 2014) (unofficial translation).
72 Article 5.
73 Article 37.

about the execution of the authorization, which neither he nor anyone in his office may divulge.[74]

Actions related to national security are subject to legislative control. The law provides for a bicameral commission, composed of three senators and three representatives, that makes specific requests of the Center for Research and National Security and Investigation, reviews the general reports, and has the ability to make recommendations regarding any topic. The center may abstain from revealing information that might endanger national security, and the commission is also obligated to maintain this reservation.[75]

In Search of a Balanced System

In light of modern technology, the Colombian regime regarding communications surveillance presents at least three problems: (i) although there is a conceptual distinction between surveillance of the radio electric spectrum and the interception of communications, in practice these activities overlap: an interception may derive from a surveillance activity, or the spectrum can be monitored during the course of an interception; (ii) in the absence of a clear definition, communications interceptions can lead to mass surveillance or the disproportionate surveillance of an individual; (iii) combined with other surveillance tools, access to user data constitutes an additional risk of fundamental rights violations.

These points converge in one form or another in definitions and controls. Regulation and jurisprudence must adequately interpret the capacity and functioning of modern surveillance schemes. But any advance in this respect will be useless if daily controls regarding surveillance ignore minimum constitutional guarantees and human rights.

I this chapter, I will begin by discussing the rights involved, particularly the right to privacy. I will then return to the proposed discussion and, finally, offer some concluding considerations.

Privacy and other threatened rights

Regardless of whether communications surveillance is undertaken in the context of a criminal proceeding or as part of the state's intelligence activities, it is in tension with the fundamental right to privacy. Thus, article 15 of the Constitution describes the interception and registry of communications as an exception to family intimacy and privacy of communications. However, the right to privacy is not the only right at risk. Habeas data and freedom of expression, to mention the most relevant, are also equally compromised.

The Colombian Constitutional Court has used different theoretical approaches to define the essential nucleus of the right to privacy and intimacy. Throughout more than twenty years of jurisprudence, the court has delineated this in spatial, visual, and informational terms, suggesting the influence of various legal traditions.

As the court recently stated, "The basic content of the fundamental right to privacy presupposes the existence and enjoyment of a space reserved for each individual that is free from intervention or arbitrary intrusions of the State and society."[76] To this spatial criteria, in the metaphorical sense, the court adds the premise of the "right to be let alone," borrowed from US doctrine:

> [C]onstitutional protection of the right to be let alone, as an essential manifestation of the right to privacy, finds support not only in phenomenon of solitude, which analyzed alone does not enrich the content of said right, but rather in the right to not be observed, and to be able to act without fear that someone, at any moment, will reveal an exclusive action or sphere of behavior.[77]

The court thus summarizes the violation of the right to privacy in three scenarios: (i) irrational intrusion in the sphere that each person has reserved for himself; (ii) the divulging of private facts; and (iii) slanted or false dissemination of personal issues that, according to the court, relate to the right to honor and a good name.[78]

Visual metaphors are less present in constitutional jurisprudence. The idea that the right to privacy is not limited to a space (home, work, one's body)—but rather also involves the individual's interest in not being observed in certain circumstances—allows for the extension of the reach of this right; the possibility to observe a person beyond his physical

74 Article 45.
75 Article 57.
76 Constitutional Court, Decision C-540 of 2012, Presiding Magistrate Jorge Iván Palacio (unofficial translation).
77 Constitutional Court, Decision C-787 of 2004, Presiding Magistrate Rodrigo Escobar Gil (unofficial translation).
78 Op. Cit. Decision 787 of 2004.

presence—including any content, information, data, or photograph that represents him or says something about him.

Additionally, observation as a violation of the right to privacy is not defined purely in terms of the action of observing. In other words, generalized surveillance and the disproportionate interception of communications are problematic not only because someone accesses information about the individual and, eventually, stores or shares it. Generalized surveillance, in itself, modifies the person's environment, makes him conscience of his own subjectivity, and denies him the voluntary confinement necessary to develop his individuality.

Benn considers that extensive observation inhibits the disposition to choose. Observation, he affirms, "brings one to a new consciousness of oneself, as something seen through another's eyes." Julie Cohen agrees, affirming that generalized observance constrains spontaneity and leads the individual toward the insipid.[79]

Constraining spontaneity and creating predictability is in fact the purpose of public surveillance policies such as closed-circuit cameras. Under the lens that observes, people behave in predetermined manners.[80] Translating these schemes, themselves questionable, to all spheres of the individual limits privacy and affects the free development of the person.

It thus becomes clear that the right to freedom of expression is also at risk when the sphere of individual privacy disappears. On one hand, the absence of a space of reclusion prohibits reflection, experimentation, the development of convictions, and interpretations of reality. On the other, the imminence of external observation requires the individual to pass his opinions through the filter of public or private mediation. Paraphrasing writer George Mangakis in his reference to penitentiary authorities' practice of reviewing inmates' correspondence, the risk is that the individual begins to control his own thoughts in light of the person observing them.[81] Put succinctly, without privacy, freedom of expression is a mere act.

79 Kang, J. Information Privacy in Cyberspace. Stanford Law Review, Vol. 50, No. 4, 1998, p. 1260. Cf. Cohen, Julie. Examined Lives: Informational Privacy and the Subject as Object. Stanford Law Review. Vol. 52:1373, 2000.

80 Cf. Cohen, J. Configuring the Networked Self. Law, Code and the Play of Everyday Practice. Yale University Press. Vol. 18:575, 2012.

81 Cf. Mangakis, G. In Coetzee, J.M. Contra la censura. Ensayos sobre la pasión por silenciar [Against censorship. Essays against the passion to silence]. Debate, 2007, p. 56.

The negation of privacy also impedes the exercise of other constitutional guarantees, such as the protection of journalists' sources, which in general is considered professional secret.[82] For the Constitutional Court, "The evident connection between professional secret and other fundamental rights strengthens, even more, the right to privacy and the inviolable mandate of private communications."[83]

Lastly, privacy has a close relationship with the right to habeas data. As discussed above, this right forms part of article 15 of the Constitution, which recognizes that all people "have the right to know, update, and rectify information collected about them in databases and files of public and private entities" and adds that "in the collection, treatment and circulation of data, the right to freedom and other guarantees consecrated in the Constitution will be respected."

Definitions and controls

During the Constitutional Court's revision of the Intelligence Law, several civil society organizations called attention to an issue that greatly motivated this book: surveillance of the radio electric spectrum requires the same constitutional guarantees as the interception of communications.

In its intervention before the court, the Ombudsman's Office argued that the statement "surveillance does not constitute interception of communications" was contrary the Constitution.[84] According to the office, any type of surveillance or monitoring of the spectrum eventually affects personal communications and therefore leads to violations of fundamental rights.

Similarly, Dejusticia and the Foundation for Press Freedom (FLIP) argued that surveillance was a form of interception: "sweeps of the electromagnetic spectrum are a direct intervention into individuals' right to privacy."[85] These organizations posited that the absence of a warrant leaves citizens defenseless regarding the privacy and safety of their personal communications.

82 Cf. Constitutional Court, decision T-298 of 2009, Presiding Magistrate Luis Ernesto Vargas.

83 Constitutional Court, decision T–708 of 2008, Presiding Magistrate Clara Inés Vargas.

84 Constitutional Court, decision C-540 of 2012, Presiding Magistrate Jorge Iván Palacio Palacio.

85 Constitutional Court, decision C-540 of 2012, Presiding Magistrate Jorge Iván Palacio Palacio.

For the court, as explained above, spectrum surveillance cannot constitute individual monitoring because it does not involve the "selection" of an individual target. Additionally, in an argument that does not give due respect to the importance of the case and the level of those addressing it, the court maintained that surveillance could not constitute an interception of private communications because the latter requires a warrant.

Of course, this reasoning does not resolve the practical dilemma. The fact that the interception of communications requires a warrant does not undermine the nature of the activity. By contrast, if we accept the affirmation that the practices are similar and compromise the exercise of fundamental rights, the logical conclusion is that they should be subject to the same legal standard.

Last January, citizens who participated in protests in Kiev, Ukraine, received the following text message in their phones: "Dear subscriber, you are registered as a participant in massive riots."[86] Cell phone companies denied responsibility, which is possible. The administration of then president Viktor Yanukovych could have requested the registries of all cell telephones connected to certain towers, a procedure known as tower dumps, or it could have used a StingRay to substitute one of these towers and obtain information on users within the zone.[87] This is to say, it used technology to "survey" the spectrum. By crossing it with the identity of subscribers, the administration can easily put together a list of those protesting. There is no reason to dismiss the idea that this could also occur in Colombia.

None of the three countries studied in chapter 3 makes the distinction that the Colombian regime does. Although the United Kingdom and Chile do not explicitly mention surveillance, it seems to be included within monitoring activities. In Mexico, by contrast, article 34 of the National Security Law explicitly includes surveillance within "communications intervention," which also includes interception.

86 Cf. Text messages warn Ukraine protesters they are 'participants in mass riot'. The Guardian, January 21, 2014. Available at: http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot (visited March 20, 2014).

87 Cf. A Lesson From Ukraine On Cell Phone Metadata. Here and Now, January 24, 2014. Available at: http://hereandnow.wbur.org/2014/01/24/ukraine-metadata-lesson (visited March 20, 2014).

If surveillance of the radio electric spectrum were subject to the same rules as interception, this would mean that surveillance would fall under judicial control. Although article 235 of the Colombian Criminal Code refers to the prosecutor's power to intercept communications "that pass through any communication network," and Decree 1704 of 2012 mentions any "origin of technology," no norm or jurisprudence develops criteria regarding the means used.

Is it legal to intercept the communications of someone through deceptive and potentially disproportionate methods, such as Trojans? What happens when the use of these mechanisms affects the target's property—for example, by harming his computer? What guarantees do users of a computer or network have when they are affected by a traffic analysis—using technology such as deep-packet inspection—aimed at intercepting the communications of just one individual? What guarantees exist to ensure that once the legal interception is complete, the surveillance devices will be deactivated?

Compared to traditional telephone interceptions and cell phone interceptions, internet surveillance is less expensive. While in cases of telephone and cell phone interceptions authorities must invest resources and often obtain the collaboration of the provider, infecting a computer with malware does not involve any cost for the person monitoring it, except for the cost of the malware. There are no incentives to end the activity. Rather, its level of invisibility and latency lends itself to keeping the channel open. Without adequate controls, interception in these terms has a beginning but does not seem to have an end.

It is thus important for authorized practices to be specifically enumerated. It is not the same to authorize a telephone interception for a month as it is to authorize the surreptitious installation of a Trojan for the same timeframe. And this difference should be clear for the individual authorizing the operation. Regarding this specific example, Mexican law, with solid criteria, establishes that in granting authorization, the judge must specify, among other things, "the type of activity authorized" and, when necessary, must include "express authorization to install or remove any type of instrument or means of intervention."[88]

As seen above, the Colombian Constitutional Court establishes that the judicial authority must verify that the means is adequate to achieve the

88 Op. Cit. National Security Law of Mexico, article 37.

ends, that the measure is the most benign possible, and that it is worth the sacrifice that it requires.[89] Nonetheless, these are general proportionality criteria proposed in a context—both regulatory as well as jurisprudential—where any mention of technology and its impact on the exercise of fundamental rights is omitted. Put another way, there is no other roadmap for interpreting these criteria from this perspective.

The imprecision and vagueness of constitutional precedent in this regard is evident. In 2008, for example, the court affirmed:

> In conclusion, the exercise of control and surveillance activities over the electromagnetic spectrum, as well as the uses that authorized intelligence bodies give to frequencies designated for assistance and national security, is limited by fundamental rights that may not be violated under the pretext of carrying out such activities. In effect, police authorities maintain the power to monitor the electromagnetic spectrum as long as they do not violate the right to privacy.[90]

Although Mexico, Chile, and the United Kingdom may have better criteria than Colombia in the application of controls, these criteria are applied within systems that lack many guarantees. In the United Kingdom, the commissioner for the interception of communications lacks teeth, and the Investigatory Powers Tribunal is a secret body.[91] In Mexico, the control is purely political, as it is in hands of a bicameral commission, similar to Chile, where there nonetheless exist two possibilities of external control by the comptroller and the courts.

In Colombia, by contrast, interception for surveillance purposes is subject to the same controls as those carried out in the development of a court proceeding. This is not the case with the monitoring of and access to user data, whose supervision and control are internal and political, in midst of absolute reserve.

In the Constitutional Court's decision that reviewed the Intelligence Law, Justice Luis Ernesto Vargas wrote a concurring opinion in which he indicated that intelligence agencies' annual reports to the president should be made publicly available, save for information that truly must be protected. Otherwise, he stated, "it entails a level of abstraction, generality, and ambiguity that conflicts with the principle of legality, as it involves the restriction of a fundamental right: information and transparency regarding the actions of administrative authorities."

Like monitoring, access to user data represents a powerful tool in terms of surveillance and tracking. Current legislation on intelligence permits the handing over of information by network service providers without a warrant. However, it is still unclear whether this addresses only metadata or also the content of communications (for example, a chat or message in a social network), in which case this is equivalent to an interception.

As stated at the beginning of this book, information regarding users' locations is saved in the historical files of service providers. By adding and processing this data, one can obtain an accurate account of what a person did during a determined period. To illustrate this point, in 2011, Malte Spitz, a politician from Germany's Green Party, sued his cell phone provider for revealing his location files for the previous six months. With this information, the newspaper *Zeit* created a detailed map of Spitz's movements.[92] In the words of technology expert Jacob Appelbaum, "cell phones are tracking devices that make calls."[93]

At one point, Colombia's ombudsman asked the Constitutional Court to declare article 44 of the Intelligence Law unconstitutional for its failure to include controls regarding foreseen activities. Using similar arguments, Dejusticia and FLIP maintained that accessing this data without judicial authorization constitutes a violation of the right to privacy and habeas data. These organizations asked the court to declare the article conditionally in accordance with the Constitution, with the understanding that any request for information must include a warrant.

However, the court declared the article constitutional. Using a conditional tone, but in reality situating the norm in the context of general intelligence principles, the court affirmed that requests for communications logs, the identification of users, and cell phone locations must be

89 Cf. Constitutional Court, decision C-591 of 2005, Presiding Magistrate Clara Inés Vargas.

90 Constitutional Court, decision T–708 of 2008, Presiding Magistrate Clara Inés Vargas.

91 Cf. Op. Cit. JUSTICE.

92 Betrayed by our own data. Zeit Online, March 26, 2011. Available at: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz (visited March 19, 2014).

93 Crocker, A. Trackers that make phone calls: Considering First Amendment Protection for Location Data. Harvard Journal of Law and Technology, Vol. 26, No. 2, 2013, p. 622.

based on criteria of reasonableness and proportionality, "such that the use of this collaboration mechanism is limited to those cases in which the information is absolutely necessary for the goals of intelligence and counterintelligence."[94]

Although Law 1581 of 2012 addresses the right to habeas data in detail, it excludes from the protection of personal data "databases and files whose purpose is national defense and security, as well as the prevention, detection, monitoring, and control of money laundering and the finance of terrorism" and "databases whose purpose and information relate to intelligence and counterintelligence."[95]

This opens a large space to create files on any citizen without providing for the ability to challenge them. In another case, the Constitutional Court addressed the risk that state intelligence files contain partial, decontextualized, and contradictory information.[96] This is in addition to the fact that service providers in Colombia save user data for five years, while in other regions, such as the European Union, such data is saved for two.[97] The excess of data in the power of an individual or the state is a risk not only for privacy or habeas data but also for someone's life. Since this is a complex issue that goes beyond the scope of this book, here I will merely mention the problem.

Massive surveillance is disproportionate surveillance

Neither judges nor legislators in Colombia are evaluating the impact that technology has on fundamental rights. In addressing questions related to communications, few or none are interested in understanding the capacity of a surveillance scheme to assess its individual impact. Therefore, any test of proportionality will be incomplete.

Although it is surprising that this absence occurs in a country with a history of illegal interceptions, it is common for courts to review new technologies after their incorporation into society. This situation is even more complicated with "unstable technologies." In contrast to cars and firearms, communications systems are in a state of constant flux.

94 Id. 3.9.45.2.

95 Law 1581 of 2012, article 2(b)(c).

96 Cf. Constitutional Court, decision T-1037 of 2008.

97 Cf. Directive 2006/24/EC of Parliament and the European Council. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (visited April 4, 2014).

In the United States, for example, the implications of telephone interceptions underwent judicial review almost six decades after the telephone was invented. Today, we need judicial decisions regarding issues such as deep-packet inspection—but it is possible that by the time a decision arrives, the problem will be another.[98]

Orin Kerr argues that leaving the task of interpreting technology to courts is an error: "Judicial decisions tend to incorporate outdated assumptions of technological practice, leading to rules that make little sense in the present or future."[99] Judges, he adds, do not have adequate information to situate cases in the broader context of technological changes.

In the US context, Kerr thus proposes that Congress assume the role of regulating technologies that are in constant flux, given that Congress can intervene at any point in time in response to a public concern or even before a negative impact. Additionally, Congress is not limited by judicial precedent or the formalism of adjudication; it can create new laws, revise them, and experiment with different incentives for public and private actors.[100]

It would be hasty to say that this proposal is equally viable in the Colombian context. On one hand, the Intelligence Law was a lost opportunity to do precisely that. On the other, with tools such as the *tutela*,[101] the Constitutional Court has used individual cases to encourage the development of public policies. To this extent, the court could assume the role of updating the interpretation of technology, with the advantage that it relates to cases that, contrary to the United States, take less time to reach the highest court. In any event, it seems that only legal reform is capable of encouraging a paradigmatic change that, to date, hasn't been triggered by the Constitutional Court.

Another way to approach monitoring technologies and their impact on fundamental rights could be by taking advantage of the precautionary

98 Cf. Op. Cit., Hosein, G. & Wilson, C.

99 Kerr, O. The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution. Michigan Law Review, 102, 2004, p. 107.

100 Cf. Id., p. 163.

101 Similar to a writ of *amparo*, the *tutela* permits any citizen to file a complaint before a court when he or she considers that his or her constitutional or fundamental rights have been violated. It is a relatively simple procedure that does not require an attorney, and courts are required to respond to *tutela*s within ten days.

principle. This principle applies largely in the context of the regulation of the environmental field, although it also has a concrete application in the field of international humanitarian law.[102] Put simply, the precautionary principle states that when an activity may threaten human health or the environment, governments should adopt precautionary measures, even in the absence of complete scientific certainty regarding potential harm.

For the court, environmental protection may be called for when it suspects that potential harm may come from technological or scientific innovations that are considered valuable "for contributing to the satisfaction of concrete human needs, encouraging commerce, private initiative and inventions, or for forming part of the exercise of liberal professions."[103]

These criteria could be extended to the tension between privacy and national security: applied indiscriminately or disproportionately, a given technology could harm privacy and other fundamental rights, in spite of being valuable for preserving national security. To this extent, the judge or regulatory body should adopt special protection measures.

Some have proposed applying the precautionary principle to information and communication technologies. Claudia Som, Lorenz Hilty, and Thomas Ruddy suggest this approach for articulating the risks and benefits of technology in general. Information and communication technologies, these authors argue, may not only interact with social practices but also change them. The incorporation of technology is a simultaneous process of cause and effect. The goal, then, is to ask oneself what precautionary measures could help avoid undesired effects.[104]

In the case at hand, the undesired effect is a legal and judicial framework that permits, and even encourages, the development of massive surveillance systems that, by definition, are disproportionate—in other words, surveillance without definitions or limits, without adequate controls, without deliberation between means and ends. Surveillance that, in practice, limits the validity of fundamental rights.

102 Cf. Constitutional Court, decision C-291 of 2007, Presiding Magistrate Manuel José Cepeda.

103 Constitutional Court, decision T-299 of 2008, Presiding Magistrate Jaime Córdoba Triviño (unofficial translation).

104 Cf. Som, C.; Hilty, L., & R. Thomas. The precautionary principle in the information society. Human and Ecological Risk Assessment, 10: 787-799, 2004.