State Communications Surveillance and the Protection of Fundamental Rights in Mexico

By Luis Fernando García
in collaboration with Katitza Rodríguez

December 2015

ELECTRONIC FRONTIER FOUNDATION

R3D
Red en Defensa
de los Derechos Digitales

Luis Fernando García is the director of Red en Defensa de los Derechos Digitales (R3D). He is also a lawyer who studied at the Universidad Iberoamericana and an LL.M candidate in the Program of International Human Rights Law at Universidad de Lund.

This report was drafted in partnership with the Electronic Frontier Foundation (EFF). We would like to thank Katitza Rodríguez, International Rights Director at EFF, for her contribution to the substantial revision of this report; and Kim Carlson and David Bogado, EFF, for their editing and formatting work.

This report is part of EFF's "Surveillance and Human Rights" project carried out in eight countries in Latin America by the Electronic Frontier Foundation, an international non-profit organization that, since 1990, has been defending freedom of expression and privacy in the digital world.

Red en Defensa de los Derechos Digitales (R3D) is a Mexican organization devoted to defending human rights in the digital world.

Table of Contents

Introduction

The right to privacy is a fundamental right that is necessary for human dignity and fundamental freedoms such as freedom of expression and freedom of association.. Unfortunately, the right to privacy has been increasingly threatened by public and private actors who seek to take advantage of technological advancements in order to interfere with the private lives of many.

Even though the use of technology to prosecute crimes and/or ensure security may pursue a legitimate aim, it is important to take into consideration that these practices often infringe greatly on human rights given that the measures are highly invasive and often require secrecy to be effective.

Moreover, the secret nature of surveillance measures poses a serious threat to individuals' dignity and to the aspirations of democratic coexistence. As such, international human rights law and constitutional doctrines have established a variety of principles that seek to curb abuse and guarantee accountability.

In Mexico, although there are conventional, comprehensive, and constitutional protections for the right to privacy, technical and legal capabilities for communications surveillance have been exponentially expanded within the last decade. Such expansions have not been accompanied by the appropriate safeguards, which, in an institutionally-weak country such as Mexico, poses a serious threat to the security of individuals, and particularly vulnerable groups, such as journalists and human rights activists.

This report outlines the constitutional and international protections of human rights related to the right to privacy in the situations of communications surveillance. It describes domestic regulations on this subject and then gives recommendations for legal reform based on the human rights standards outlined in the International Principles on the Application of Human Rights to Communications Surveillance.[1]

I.
Constitutional Legal Framework for the Protection of Human Rights against State Communications Surveillance in Mexico

Communications privacy is protected by Article 16 of the Constitution of Mexico. Specifically, paragraphs 12 and 13 provide for what has been characterized by the Mexican constitutional interpretation bodies as the inviolability of communications:

> *"Private communications are inviolable. The law shall punish any act that interferes with the freedom and privacy of communications, except when they are voluntarily delivered by one of their participants. The judge shall assess their scope, as long as they contain information related to the commission of a crime. Under no circumstances will communications violating the duty of confidentiality established by law be allowed.*
>
> *The federal judicial authority shall, exclusively and upon the request of the federal authority appointed by law or the public official of the Public Prosecutor's Office of the pertaining federative entity, be able to authorize the interception of any private communication. In order to do so, the competent authority shall establish and justify the legal reasons of the request, specifying the type of interception, its subjects and its duration. The federal judicial authority shall not be able to grant these authorizations in electoral, tax, commercial, civil, occupational or administrative cases, nor in the case of communications between the accused and his/her counselor."*

The Constitution establishes special safeguards relative to the measures that interfere with the right to inviolability of communications, such as requiring a federal judicial order to intercept private communications; establishing a legal basis and justification for intercepting communications; requiring transparency surrounding the request (the type of interception, the subject, and the duration); and limiting involvement to only federal authorities appointed by law or public officials of the Public Prosecutor's Office.

The Supreme Court in Mexico (*SCJN, in Spanish*) has interpreted this provision in *Amparo en Revision 1621/2010* and the Thesis Contradiction 194/2012 clarifying that the constitutional protection of private communications includes all existing forms of

communication including those which may result from technological advances, like communications via Internet.[2]

Moreover, the SCJN explicitly stated that constitutional protections relative to the inviolability of communications may involve not only the content and the process of communication, but also the data identifying the communication:

> *"(...) With the purpose of guaranteeing the secrecy of all communicative processes, it is essential for the data external to the communication to be protected as well. Even though it is true that this data is not referred to the content of communication, it usually gives information about the circumstances under which the communication has taken place, thus affecting–directly or indirectly–the privacy of those who participate in the communication. This data, called "communications traffic data," shall be the object of study of the interpreter, in order to determine whether their interception and unlawfulness are contrary to the fundamental right in each individual case. Hence, by way of example, the call logs of a telephone network user, the identity of the participants, the duration of the phone call or the identification of an IP address, carried out without the necessary guarantees for the restriction of the fundamental right to secrecy of communications, may lead to their infringement."*

Taking this provision into account, the SCJN has considered that accessing and analyzing data stored on a mobile phone without a judicial order is an infringement on the right to inviolability of private communications.[3]

According to the SCJN, there is a violation of the right to privacy at the moment of listening to, recording, storing, reading or registering a private communication without the participants' consent, regardless of the possibility of subsequent dissemination of the contents of the intercepted communication.[4]

This is why the SCJN considers that an email has been intercepted—in such a way that infringes upon the right to inviolability of communications—from the moment that the password of an account has been taken without judicial order or the user's consent regardless of whether the content of the email was analyzed.[5]

The SCJN has interpreted that the constitutional protection of communications is extended beyond the moment in which the communication takes place. As such, the Constitution protects individuals against communication interception in real time, as well as subsequent interferences on physical devices that store the communication.[6]

Thus, at the regulatory level, the Constitution grants comprehensive protections for the right to inviolability of communications. However, the precedents of communications surveillance are scarce in constitutional case law, so the content and scope of this right is still under discussion.

For example, the SCJN's decision regarding the complaint of unconstitutionality 32/2012,[7] in which the greater part of the Supreme Court considered that it is constitutional to allow the Public Attorney's Office (*PGR, in Spanish*) to monitor the geolocation of a mobile phone in real time, without the need for a federal judicial order. Although the majority in this case considered that the surveillance did interfere with the individuals' right to privacy, the precept was validated under the imposition of minimum safeguards through a "conforming interpretation."

Regardless of the decision, the provisions analyzed by the Supreme Court have been repealed by others that include even fewer safeguards. Thus, the SCJN has another opportunity to review its arguments and analyze the constitutionality of the new provisions on geolocation in the Criminal Procedure Code when making a decision about the unconstitutionality complaints (*acciones de inconstitucionalidad in Spanish)* 10/2014 and 11/2014, which are on their way to being resolved.

I.1 Normative Power of International Human Rights Treaties Affected by State Communications Surveillance in Mexico

The Mexican legal system has been substantially modified in the last few years, and human rights have been at the heart of it. Particularly, the reform of Article 1 of the Constitution and others, published in the Diario Oficial de la Federación on June 10, 2011, made changes that aim to strengthen the normative prevalence of human rights.

One of the most important changes reflected in Article 1 of the Constitution is the constitutional acknowledgment and acceptance of international human rights treaties. The Constitution also establishes *pro personae principle*, which establishes that provisions should be interpreted in the most favorable way for human rights. This means that, in general, any hierarchical relationships between the "sources of law" (*fuentes del derecho*) that recognizes human rights would be eliminated.

Similarly, the constitutional reform obliges all authorities to promote, respect, protect, and guarantee human rights in accordance with the principles of universality, indivisibility, interdependence, and progressiveness.

Since the constitutional reform, the SCJN has elaborated a doctrine recognizing constitutional and international sources of human rights law as international components

of the same catalog of laws that the authority and the Mexican legal system must comply with.[8]

This means that the human rights recognized in the Constitution and in international treaties such as the International Covenant on Civil and Political Rights and the American Convention on Human Rights, including their interpretation by the authorized bodies, make up a "parameter of constitutional consistency" with no hierarchy among their provisions. In case of antinomy, the most favorable regulation is followed in accordance with the *pro personae* principle.

Additionally, the consolidation of the "parameter of constitutional consistency" (*parámetro de regularidad constitucional in Spanish*), derived from the constitutional reform of the writ of Amparo (*Acción de Amparo in Spanish*), published on June 6, 2011, grants the possibility of controlling the constitutionality of all regulations and acts of authorities through Amparo proceedings. This way, individuals have a powerful tool to combat the violations of their human rights, even with the direct application of international human rights law.

I.2 Safeguards for State Communications Surveillance in International Law

International human rights law has also elaborated on its content and scope of the right to privacy related to surveillance.

Although there is not a significant amount of decisions on the subject in the Inter-American Human Rights System, there are some precedents that widely protect the right to privacy of communications. For instance, in the *Case of Escher vs. Brazil*, the Inter-American Court of Human Rights (IACHR) interpreted Article 11 of the American Convention on Human Rights (ACHR) (which recognizes the right to non-arbitrary interference of communications) as protecting both the content of communications and the *metadata* which identifies such communication:

> *"Article 11 applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call by taping the conversation. In brief, the protection of privacy is manifested in the right that individuals other than those conversing may not illegally obtain information on the content of the*

telephone conversations or other aspects inherent in the communication process, such as those mentioned."

This confirms what was adopted by the Mexican Judicial Branch, in the sense that the content of communications given by the parameter of constitutional consistency is protected, along with any other element of the communication process, like *metadata*, which is also protected constitutionally and conventionally.

On the other hand, both the Inter-American Commission on Human Rights, through the Special Rapporteur for Freedom of Expression, and the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression have stated that it is important to adopt the appropriate safeguards to inhibit the risks of abuse of communications surveillance measures, since they represent serious interferences on the right to privacy and the right to freedom of expression.

In this regard, the UN Special Rapporteur for the Promotion and Protection of the Right to Freedom of Expression and the Special Rapporteur for the Freedom of Expression of the Inter-American Commission on Human Rights note in the Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression that:

"States must guarantee that the interception, collection and use of personal information (...) be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged." [9]

Similarly, the above-mentioned international mechanisms of protection have stated that in the context of covert surveillance activities, the law must be clear enough to provide the public with the appropriate explanation about the conditions and circumstances in which authorities have the power to resort to such measures. [10]

Furthermore, in light of the risks of abuse that any secret surveillance system poses, the measures must be based on a particularly precise law, since the available technology to execute these activities is constantly becoming more sophisticated. [11] Thus, in order for covert surveillance measures to comply with the *necessity test* related to the restrictions to the right to privacy, it is essential that there be measures inhibiting inherent risks of abuse.

International bodies, such as the European Court of Human Rights, have repeatedly emphasized in their case law that the existence of appropriate and effective safeguards is

crucial in complying with the necessity and proportionality criteria that is stipulated in the laws that allow for the invasion of privacy.[12]

Accordingly, the importance of the effective guarantees against the abuse of electronic covert surveillance measures has been recently highlighted by the United Nations General Assembly (UN),[13] the UN Special Rapporteur for the Right to Freedom of Expression and Opinion,[14] the UN High Commissioner for Human Rights,[15] the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights,[16] and also by organizations of the civil society and experts who have gathered best practices derived from compared case law and doctrine and have drafted the International Principles on the Application of Human Rights to Communications Surveillance.[17]

A fundamental safeguard used to inhibit inherent risks of abuse of surveillance measures is judicial control. Prior or immediate judicial control of covert surveillance measures that invade individuals' privacy has been recently emphasized by the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, who has stated that:

> *"Decisions to undertake surveillance activities that invade the privacy of individuals must be authorized by independent judicial authorities, who must state why the measure is appropriate for the accomplishment of the objectives pursued in the specific case; whether it is sufficiently restricted so as not to infringe upon the right in question more than necessary; and whether it is proportionate in relation to the interests pursued."*[18]

The existence of independent oversight mechanisms and transparency of surveillance activities are other measures that have been identified in international law as appropriate safeguards for inhibiting abuse of covert communications surveillance measures.

For instance, in the resolution "The right to privacy in the digital age," adopted by consensus by the members of the UN General Assembly on December 18, 2013, it is stated that States should "establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."[19]

In turn, the UN Special Rapporteur on the Right to Freedom of Expression and Opinion indicated, in his report, the dangers of communications surveillance:

> *"States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved*

and rejected, a disaggregation of the requests by service provider and by investigation and purpose.

States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance. (...)"[20]

Similarly, in the Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression,[21] the UN Special Rapporteur on the Right to Freedom of Expression and Opinion and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) stated that:

"All persons have the right to access information held by the state, including information having to do with national security. The law may establish specific exceptions as long as those exceptions are necessary in a democratic society. the law must ensure that the public can access information on private communications surveillance programs, including their scope and any regulation that may be in place to guarantee that they cannot be used arbitrarily. Consequently, states should, at the very least, make public information regarding the regulatory framework of surveillance programs; the entities in charge of their implementation and oversight; the procedures for authorizing, choosing targets, and using the data collected; and the use of these techniques, including aggregate information on their scope. At all times, the state must maintain independent oversight mechanisms that are capable of ensuring program transparency and accountability. (...)

The state has the obligation to divulge information regarding the existence of illegal programs of surveillance of private communication broadly. This duty must be satisfied given due consideration to the rights of the persons affected. In every case, states must carry out exhaustive investigations to identify and punish those who pursue these types of practices and report in a timely fashion to those who may have been victims of them."

This was reaffirmed by the Special Rapporteur for Freedom of Expression of the IACHR, who stated in her "Report on the Freedom of Expression and the Internet" that:[22]

"States should disclose general information on the number of requests for interception and surveillance that have been approved and rejected, and

should include as much information as possible, such as—for example—a breakdown of requests by service provider, type of investigation, time period covered by the investigations, etc."

Another document that recognizes that States are compelled to guarantee transparency with respect to surveillance programs of national security purpose is the Global Principles on National Security and the Right to Information, (Tshwane Principles)[23] which states in Principle 10 the "Categories of Information with a High Presumption or Overriding Interest in Favor of Disclosure:"

"E. Surveillance

(1) The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.

(2) The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.

(3) The public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.

(4) These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance."

Moreover, another appropriate safeguard to guarantee the necessity and proportionality of surveillance measures is to notify those affected. This right to notification has been recognized, for instance, by the UN Special Rapporteur on the Right to Freedom of Expression and Opinion:

"Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath."[24]

The right to notification has also been recognized by the European Court of Human Rights, which established in the *Case of Ekimdzhiev vs. Bulgaria* that once surveillance has stopped and the necessary time has elapsed for the legitimate surveillance aim not to be at risk, those affected must be notified without delay.[25]

Thus, the principles of legality, adequacy, necessity, and proportionality have been elaborated in the international human rights law for the adoption of surveillance measures that covertly invade private communications.

II.
Legal Provisions Dealing with the Regulation of State Communications Surveillance Activities in Mexico

In Mexican federal legislation, there are several authorities that have the power to intercept private communications and, in general, conduct covert surveillance activities.

Institutional Framework—Authorities with the Power to Intercept Private Communications in Mexico	
The Public Prosecutor's Office (Public Attorney's Office) + Procurators' Offices / Prosecution Offices of the 31 federative organizations and the Federal District.	Article 16 of the Constitution establishes that public prosecutors may intercept private communications for the investigation of crimes, with prior approval from the federal judicial authority. The Criminal Procedure Code and the 32 local criminal procedure codes, which shall be replaced by the National Criminal Procedure Code, allow public prosecutors to intercept private communications and order data retention, obtain devices' geolocation in real time, and access the metadata of communications, without a court order.
	Article 16 of the Constitution. National Criminal Procedure Code (Articles 291 – 303.) Federal Criminal Procedure Code (Articles 278 a – 278 b.) Local Criminal Procedure Codes (31 States + Federal District.) Federal Telecommunications and Broadcasting Law (Articles 189 – 190.) General Law to Prevent and Punish Crimes of Abduction (Article 24.) Federal Law against Organized Crime (Articles 15 – 28.)
National Security Commission (Federal Police)	The Federal Police Law grants the Federal Police power to surveil communications, exclusively when there is federal judicial authorization noting the existence of sufficient evidence proving that one of the crimes listed in Article 51 of this law is being plotted.
	Federal Police Law (Articles 48 – 55.) Federal Telecommunications and Broadcasting Law (Articles 189 – 190.)
Center for Investigations and National Security (Executive Branch)	The National Security Law empowers the Center for Investigations and National Security to intercept private communications, with prior federal judicial authorization, in cases that have an "imminent threat" to national security.
	National Security Law (Articles 33 – 49.) Federal Telecommunications and Broadcasting Law (Articles 189 – 190.)

Notwithstanding the above, in July 2015, it was revealed that, through the publication of internal documents of the Italian company Hacking Team S.R.L., a number of Mexican

state and federal authorities had purchased malicious spy software[26] without the necessary constitutional or legal powers to intercept private communications.[27]

II.1 Regulations on State Communications Surveillance for the Prevention and Investigation of Crimes

In Mexico, the Public Prosecutor's Office (PGR) is in charge of investigating crimes, as well as the procurators' offices of each of the 32 federative organizations. The Public Prosecutor's Office (PGR) has the power to conduct covert surveillance activities, according to the Federal Criminal Procedure Code (CFPP, in Spanish) amended in 2009.[28]

The CFPP, which is still in force at the federal level, outlines in Article 278a that "the concessionaires and providers of telecommunications and Internet services shall be compelled to collaborate with the authorities to obtain [private communications] when requested." Similarly, Article 278b explains in detail the procedures that must be followed to conduct the interception of private communications. This article points to the need of judicial authorization, which shall be granted "when there is sufficient evidence suggesting responsibility for the commission of a serious crime."

Furthermore, the CFPP stipulates that the request, and its appropriate authorization, must specify the aspects of the interception that will be carried out, such as: the legal precepts on which it is based, the reasons why it is necessary, the type of communications that will be intercepted, the subjects and the places that will be intercepted, and the period during which the interception will be conducted (which must not exceed six months.) The judge must periodically verify compliance with the terms of authorization, and in the event a case is dismissed, the collected communications must be presented before the judge and destroyed in his/her presence.

Similarly, the laws on abduction passed in 2010[29] and on organized crime passed in 2007[30] grant the PGR the ability to intercept private communications. The prosecution offices of each of the 31 Mexican States and of the Federal District generally possess the power to intercept private communications pursuant to state legislation.

Likewise, Article 133c of the CFPP allows the PGR to request geolocation data in real time from the telecommunications and Internet service providers, by its own initiative or electronic means. In other words, during an investigation of organized crime, crimes against human health, abduction, extortion, or other serious threats, the CFPP allows delivery of geographical location data of mobile communication devices in real time without judicial authorization.

The constitutionality of this article was challenged by the complaint of unconstitutionality 32/2012, filed by the National Commission on Human Rights. However, the SCJN ruled it constitutional based on the interpretation that this article only grants this power during emergencies related to those specific crimes and that it is an ephemeral measure, meaning it stops at that exact moment and does not allow for the sustained monitoring of the location data.

Notwithstanding the above, the National Criminal Procedure Code (CNPP) was published in March 2014, and it intends to replace the Federal Criminal Procedure Code, the 31 State Codes and the Federal District Code. This National Criminal Procedure Code will be rolled out gradually by, the latest, June 2016, in the several federative organizations and at the federal level. The CNPP reaffirms the legal authority to surveil granted to law enforcement authorities (*procuración de justicia in Spanish*) as stated in the Federal Code, but with some changes.

Article 291 of the National Code, by way of example, clearly establishes that the interception of private communications, and the necessity to obtain a judicial authorization, involve not only the content of communications, but also the data that identifies the communication—m*etadata*—either in real time or after the communications has taken place.

Nonetheless, the National Criminal Procedure Code is less clear than the Federal Criminal Procedure Code when referring to the appropriateness of the request only when there is sufficient evidence of participation or probable cause.

Article 303 of the CNPP also grants the ability to monitor geographical location of communication devices in real time without judicial authorization and it extends this ability to any kind of investigation, instead of a closed list of crimes, as the CFPP does.

As previously mentioned, the constitutionality of this article shall be analyzed in the decisions of the Complaints of Unconstitutionality 10/2014 and 11/2014, filed by the National Commission on Human Rights and the Federal Institute for Information Access and Protection of Data (IFAI, in Spanish). IFAI will rule on the matter soon. This ruling may generate a precedent different from the one already issued by the above-mentioned Complaint of Unconstitutionality 32/2012, since the provision of the CNPP substantially modifies and extends the scope of the measure. Thus, the considerations mentioned by the SCJN are not fully applicable.

On the other hand, the CNPP includes the ability to order the retention of data in networks, computer systems, or devices without a court order. Besides, it does not add the necessary safeguards, such as an independent oversight mechanism, transparency based

upon statistical information on surveillance requests, or notification to the individual affected by the surveillance measure.

In December 2014, the Senate of the Republic passed a reform of Articles 291 and 303 of the CNPP in which the need for a federal judicial authorization is firmly established in order to conduct surveillance related to geographical location of mobile communication devices in real time and to access data stored by the telecommunications companies, Internet service providers, and application providers. This reform still requires the endorsement of the House of Representatives, which is still pending.[31]

On the other hand, the laws allow several federal law enforcement authorities to conduct covert surveillance activities.

The Federal Police Law was passed in 2009. It empowers the Federal Police to intercept private communications to prevent certain crimes.[32] Article 48 of this law explicitly states that the judicial authorization for the interception of private communications shall be granted "only upon the request of the Commissioner General, when there is sufficient evidence suggesting the existence of the organization of [...] crimes," which are listed in Article 51 of this law.

Similarly, Article 8, section XXVIII empowers the Federal Police to request, with prior judicial authorization, any type of information, including the geolocation of mobile communication devices in real time from the service providers and operators of telephone services and from all telecommunications companies in order to prevent a crime.

II.2 Communications Surveillance in Telecommunications Legislation

Since most communications are carried out via the services provided by private companies (telephone or Internet companies), the State usually requires their cooperation to conduct surveillance. This applies to both cases: criminal investigations and protecting national security through the use of intelligence activities.

In this regard, the Federal Telecommunications Law was amended in 2009[33] to require telecommunications companies to retain *metadata* such as type of communication, services used, origin and destination of communications, date, time, and duration of communications and even geographical location of communication devices. The obligation to retain data lasts for twelve (12) months and applies to all users of telecommunications companies' services.

The Federal Telecommunications Law allowed the Public Prosecutor's Office and the federative organizations procurators to access data retained by telecommunications companies without judicial authorization in order to investigate serious crimes.

In 2014, the Federal Telecommunications Law was replaced by the Federal Telecommunications and Broadcasting Law (LFTR, in Spanish), which significantly expanded the State's surveillance powers and increased the telecommunications service providers' obligations to cooperate in matters related to State communications surveillance.

Article 189 of the LFTR vaguely establishes the general obligation for telecommunications companies and applications and content service providers to comply with all "written requests that are well-founded and justified by the competent authority." The LFTR identifies "competent authorities" in general terms, as Mexican security units and the Attorney General Offices (*instancias de seguridad y procuración de justicia in Spanish*), without identifying specifically who these authorities are.

For example, several authorities have considered that this article of the LFTR sufficiently empowers these authorities to use covert surveillance tools, and that this power does not need to be specified in another law. For instance, the "Financial Intelligence Unit" of the Ministry of Finance and Public Credit is considered to be a "national security unit" pursuant to Article 189. The guidelines for collaboration in national security (*bases de colaboración in Spanish)*, acknowledge that the Ministry of Interior and the Ministry of Finance and Public Credit is a national security unit."[34] Furthermore, there are reports which claim that authorities, like the National Electoral Institute, may have sent these types of requests in order to access the personal data of users of telecommunication services.[35]

Article 190, Section I of the LFTR imposes obligations on the companies to "collaborate with the security proceedings, law enforcement procedures, and the obtaining of geographical location of the mobile communication devices in real time." The above means extending the power to access "geolocation" to authorities who do not have this power—nor did they have it in the past—in an enabling law, such as the "security proceedings" or the "law enforcement instances," which are not defined neither in the LFTR or in any other law.

Article 190, Section II of the LFTR establishes a requirement to retain the data of telecommunications users. This power already exists. It was included in the now-abrogated Federal Telecommunications Law. However, Article 190 of the LFTR extends the retention period to up to 24 months.

Telecommunications companies' obligations specifically require the following data to be retained:

a) The user's name, business name or corporate name and address;

b) Type of communication (voice transmissions, voicemail, conference, data), or other services (including call forwarding and transfers), or messenger or multimedia services used (including the services of short messaging, multimedia and advanced services);

c) Data showing the necessary information to track the origin and destination of mobile communications: destination number, types of line service –lines with a contract or a flat rate plan, like the lines of prepaid credit;

d) Data to determine the date, time and duration of the communication, as well as the messaging and multimedia service;

e) Data about the date and time of the first service activation and localization tag (Cell ID);

f) When appropriate, the identification and technical characteristics of the device, including, among others, the international ID codes of the subscriber and the manufacturing of the device;

g) The geographical position of the lines, and

h) The obligation to store data shall begin since the date in which the communication is produced.

The company must keep data for 12 months "in systems that allow the access by and delivery to the competent authorities in real time, through electronic means." After this time period, the data shall be kept for 12 additional months and be delivered to the authority that requests it within 48 hours following the request.

For its part, Article 190, Section III of the LFTR imposes the obligation to deliver the retained data to "the requesting authorities referred to in Article 189 of this Law." As stated above, the concept of "security proceedings" is highly ambiguous. Moreover, it is important to mention that the need for judicial authorization is not explicitly established.

The Federal Telecommunications Institute (IFT, in Spanish), in accordance with Article 189 of the Federal Telecommunications and Broadcasting Law, is still in the issuance process of the "Guidelines for Collaboration in Security and Justice." In November 2014, the IFT published a draft that was subject to public consultation. Even though this draft does not amend the constitutional problems of the law, it recognizes some safeguards related to transparency.

In particular, the fourteenth guideline of this draft suggests the following obligations:

> *FOURTEENTH: The concessionaires and those authorized must deliver every January and every July a semi-annual report related to the application of these guidelines to the Federal Telecommunications Institute. This report shall contain the total number–by Designated Authority–of requests for geolocation information and communications data records, braking them down into the communications received, processed and delivered.*
>
> *The Institute shall request from the Designated Authorities a semi-annual report (in January and July) related to the number of requests for geolocation and data records, distinguishing between those were rejected and the ones in which information was received in due time.*
>
> *The information contained in these reports shall be published on the Institute's website on the basis of Article 7 Section XVII of the Federal Law for Transparency and Access to Public Government Information.*

Similarly, the General Law in Transparency and Access to Public Information was passed by Congress in April 2015. It includes the following transparency obligations related to surveillance:

> *Article 70. The Federal Law and the Federative Organizations Law shall stipulate that the designated subjects are compelled to make information about, at least, topics, documents and policies available to the public, and they shall keep it updated in the appropriate electronic media, pursuant to their powers, attributions, duties and social objectives, accordingly. The types of information about topics, documents and policies are the following:*
>
> *XLVII. For statistical purposes, the listing of requests made to the telecommunications companies and Internet applications and service providers for the interception of private communications, the access to communications logs and the geolocation of communication devices in real time containing the object, temporal scope and legal foundations of the request, as well as, when appropriate, the acknowledgment of the existence of a pertaining judicial authorization.*

II.3 State Communications Surveillance in Intelligence and Counterintelligence Legislation

In addition to the regulations related to the prevention and investigation of crimes and to telecommunications legislation, legislators have provided for the possibility of restricting individuals' rights through communications surveillance measures in the context of intelligence and counterintelligence activities.

The National Security Law empowers the Center for Investigations and National Security (*CISEN, in Spanish*) to intercept private communications in the cases of "imminent threat to national security."[36] Article 5 of this law gives an extremely broad definition of the "imminent threats to national security":

> *Article 5.- For the purposes of this Act, threats to National Security shall be:*
>
> *I. Acts aimed at committing espionage, sabotage, terrorism, rebellion, treason, genocide, against the United Mexican States within its territory;*
>
> *II. Acts of foreign interference in domestic affairs that may cause harm to the Mexican State;*
>
> *III. Acts that prevent the authorities from acting against organized crime;*
>
> *IV. Acts aimed at undermining the unity of the parties comprising the federation, as stated in article 43 of the United Mexican States Political Constitution;*
>
> *V. Acts aimed at hindering or blocking military or naval operations against organized crime;*
>
> *VI. Acts against aviation security;*
>
> *VII. Acts directed against diplomatic personnel;*
>
> *VIII. All acts aimed at carrying out the illegal traffic of nuclear materials, chemical, biological, and conventional weapons of mass destruction;*
>
> *IX. Unlawful acts against maritime navigation;*
>
> *X. Any act involving the financing of terrorist acts and organizations;*
>
> *XI. Acts aimed at hindering or blocking intelligence or counterintelligence activities; and*
>
> *XII. Acts aimed at destroying or disabling strategic infrastructure or the one essential to provide goods or public services.*

Even though both the Federal Police and the CISEN need to have a judicial authorization to conduct these measures, the orders do not establish other safeguards against abuse such as an independent oversight mechanism, transparency measures (aggregate data of number of surveillance requests) or prior or subsequent notification measures.

Furthermore, the law restricts access to information with respect to national security in a broad and vague manner. Particularly, Article 51 of the National Security Law defines confidential information as "that whose application means the disclosure of regulations, procedures, methods, sources, technical specifications, technology or equipment useful to produce intelligence for National Security, regardless of the nature or origin of the documents containing it," as well as "that whose disclosure may be used for upgrading or strengthening a threat."

As such, the institutional safeguards capable of overseeing national security proceedings are extremely scarce, which increases the risks of abuse of power.

II.4 Legal Remedies and Penalties against the Abuse of State Surveillance Measures

Amparo proceedings, regulated by the Amparo Law, are the appropriate remedy to redress violations of recognized human rights, both in the Constitution and in international regulations on human rights. In this regard, it is possible to use this remedy to challenge acts or regulations infringing upon the right to privacy and the inviolability of private communications.

Not withstanding, there are some barriers that impede the full effectiveness of Amparo proceedings. For instance, the Constitution and Amparo Law regulate these proceedings in a way in which its effects are targeted, that is, they only protect the person resorting to Amparo proceedings. Consequently, in the case of surveillance regulations that do not comply with the standards for the protection of the right to privacy, a particular sentence on Amparo proceedings merely protects the plaintiff and not the general population.

Likewise, judicial sentences that do not consider the legal standing (*locus standi)* to challenge the regulations establishing communications surveillance measures still persist, since it is necessary to prove the application of such regulations to the plaintiff, so that he or she may demonstrate a current and actual infringement.

Given the secret nature of covert surveillance practices, it is impossible to be able to prove when they are improperly carried out. However, there are some precedents for a person to challenge covert surveillance measures, without even having to prove a particular instance, since these regulations, due to their mere existence, affect the plaintiffs' legal sphere.[37]

On the other hand, the Federal Law on the Protection of Personal Data Held by Private Parties provides individuals with some mechanisms so that they can protect their right to privacy of personal data when it is held by private parties by recognizing the right to Access, Rectification, Cancellation and Objection. This law provides for a verification process, through which the National Institute for Access to Information and Protection of Data (*INAI, in Spanish*) may verify compliance with the law and impose sanctions when there's a failure to comply.

Finally, Article 177 of the Federal Criminal Code deems the interception of private communications without authorization issued by a competent judicial authority a serious crime, punishable by imprisonment for a period ranging from six to 12 years. However, there are no public precedents of the application of this criminal offense to anyone in Mexico.

III.
Does Mexican Legislation Comply with the International Human Right Standards Regarding State Communication Surveillance?

The highest standards for the protection of the right to privacy in relation to State communications surveillance recognized in case law and doctrine of international human rights bodies and courts around the world have been gathered and drafted into the "International Principles on the Application of Human Rights to Communications Surveillance."[38]

The thirteen principles of this document are:

Legality

Any limitation to human rights must be prescribed by law. This should consist in a publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of the scope of communications surveillance measures.

Legitimate Aim

Laws should only permit communications surveillance to achieve legitimate aims and this must not be applied in a discriminatory manner.

Necessity

Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or when it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.

Adequacy

Communications surveillance must be appropriate to fulfill the specific legitimate aim identified.

Proportionality

Communications surveillance must only be authorized by an independent judicial authority when there is a high degree of probability that a serious crime or specific threat to national security may be carried out. The surveillance measures used must be the least invasive option, which entails that the information accessed will be confined to that which is relevant and material to the achievement of the legitimate aim that justifies the authorization for limited time periods.

Competent Judicial Authority

Communications surveillance measures must be previously—or immediately and retroactively in emergencies—authorized by a competent judicial authority that is impartial and independent.

Due Process

Decisions authorizing communications surveillance measures must guarantee due process. This implies that, when trying to achieve a legitimate aim and, in particular, when protecting a person's life, and the secrecy or immediate application of the measure is necessary, there are other measures guaranteeing the protection of the interests of those affected. Everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law. In emergencies, retroactive authorization must be sought within a reasonably practicable time period.

User Notification

Those whose communications are being surveilled should be notified of a decision authorizing communications surveillance and must have access to the information that shall be or has been obtained. Delay in notification is only justified when the purpose of authorized communications surveillance is jeopardized or when there is an imminent risk of danger to human life.

Transparency

The State should periodically publish statistical information on the covert surveillance measures conducted. At least, it should publish the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose.

Public Oversight

States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the

authority to access all potentially relevant information about State actions in order to assess whether the State is making legitimate use of its lawful capabilities of communications surveillance.

Integrity of Communications and Systems

States should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems which may compromise the security of communications and devices. Indiscriminate and massive retention of users' data must not be demanded, nor must the right to freedom of expression be compromised by any obligation of identification or prohibitions as regards the use of encryption tools and others to protect individuals' identities and security, their communications and their devices.

Safeguards for International Cooperation

Whenever there is a need to seek international assistance to conduct surveillance measures, States may turn to the mutual legal assistance treaties (MLAT), which shall not be used to circumvent domestic legal restrictions on communications surveillance.

Safeguards against Illegitimate Access and Right to Effective Remedy

Illegal communications surveillance by public or private actors must be criminalized through sufficient and significant civil and criminal penalties. Whistleblowers must be protected by law against any legal consequence that their failure to comply with their duty of secrecy may bring about.

Legislation regulating communications surveillance in Mexico has been presented in the previous chapter. It does not comply with the constitutional and international human rights standards gathered by the 13 Principles mentioned. Therefore, it is essential to adopt, at least, the following legal reforms:

III.1 State Communications Surveillance for the Administration of Justice

The National Criminal Procedure Code recognizes that the interception of private communications requires a federal judicial authority, even to obtain the data identifying the communication. Nonetheless, the reform passed by the Senate, which is awaiting approval from the House of Representatives, establishes an exception for obtaining a federal judicial authorization. Particularly, the draft suggests the following addition to Article 291:

> *"A judicial authorization shall also be required in the cases of data extraction, which consists in obtaining private communications, data identifying private communications, as well as the information, documents, text, audio, image or video files stored in any device, accessory, electronic apparatus, computer equipment, storage device and all things that may contain information, including the data stored in the platforms or centers related. However, in case these are located in the place of the plausible commission of the crime and when no individual has been arrested, the Public Prosecutor's Office shall be able to order data extraction without the need for a pertaining judicial authorization."*

The last sentence of the paragraph that is intended to be added to the CNPP is an exception that contradicts the prior judicial authorization principle. In this regard, in the event this addition to Article 291 is passed, the constitutional and international standards recognized in the judicial authorization principle would be clearly circumvented. Thus, this addition should not be passed by the House of Representatives.

Similarly, Article 301 imposes on concessionaires of telecom services, companies, and any media or system owner that may be susceptible to interception obligations of collaboration are vague and too large in scope:

> *Article 301. Collaboration with the Authority*
>
> *The concessionaires, companies, and other media or system owners susceptible to interception must efficiently collaborate with the competent authority for the ease of the acts of investigation, pursuant to the applicable provisions. Moreover, they shall have the essential technical capabilities required by the judicial authority in order to carry out an order of interception of private communications.*
>
> *Failure to comply with this order shall be punishable according to the criminal applicable provisions.*

This power is too broad and may seriously compromise the security and integrity of communications and systems. Clear limits to the types of collaboration must be set, and, in all cases, must always be ordered by a judicial authority, not by the Public Prosecutor's Office.

The above-mentioned article (301) must be modified to limit the collaboration with the authority. In doing so, the development of surveillance capabilities or any other measure that may compromise the security and integrity of devices and systems is not a legitimate collaboration method.

In addition, Article 303 allows the Public Prosecutor's Office to order the geolocation in real time without judicial authorization involving any type of crime. Furthermore, the Office may request, without judicial authorization, the preservation of data stored in networks, systems or computer equipments, for up to 90 days in crimes related to or committed against digital media.

A reform passed by the Senate, but awaiting approval of the House of Representatives, lays down the general need for prior judicial authority for geolocation in real time. This reform also requires an immediate and retroactive judicial authorization in cases in which a person's life or physical integrity is at risk, or the object of the crime is in jeopardy, as well as in cases related to abduction, extortion, and organized crimes.

Although this represents a progress that should be passed by the House of Representatives, according to the standards set by the National Supreme Court of Justice, the deployment of this tool must be limited to the investigation of particularly serious crimes, which must be specified in the law. Apart from passing the draft of this fragment of Article 303, it should specify what types of crimes it is possible to conduct this surveillance measure.

Similarly, the Senate's draft limits the subjects compelled to follow orders for the preservation of data to telecommunications concessionaires and it would require judicial authorization to validate these orders. Therefore, this section must be passed, although it would be useful to explicitly state in the law that data preservation orders must be specific and not be indiscriminate or massive.

III.2 State Communications Surveillance for the Prevention of Crimes and the Protection of National Security

The legislation that grants surveillance powers for the prevention of crimes or the protection of national security, such as the Federal Police Law or the National Security Law, as well as the legislation specialized in abduction and organized crime, must establish in a clear, precise, and detailed manner the cases and circumstances in which the Federal Police or the Center for Investigations and National Security (CISEN) may carry out surveillance activities.

Particularly, these authorities should only be able to conduct surveillance a crime or threat to national security is real, current and imminent based on evidence. aim is When the aim is general prevention, surveillance measures must not be authorized.

In the case of national security, the law must establish accurately and specifically the cases that represent threats to national security, which must be understood as those which truly

pose a demonstrable risk to territorial integrity and the existence of the State. Thus, it is not sufficient to justify communications surveillance under the concept of "collection of intelligence."

The authorities capable of conducting surveillance activities must be explicitly and exhaustively specified. Particularly, according to Article 16 of the Constitution, only the authorities appointed by law can carry out surveillance activities with purposes different from law enforcement. Consequently, the police departments of federative organization shall not have the power to conduct surveillance autonomously, except when working under the Public Prosecutor's Office. Likewise, the military shall not be able to carry out communications surveillance activities during peacetime.

The Federal Telecommunications and Broadcasting Law should explicitly specify the authorities empowered to request collaboration with surveillance activities from the telecommunications concessionaires. Similarly, the Federal Telecommunications Institute must establish the explicit identification of the authorities entitled in the "Guidelines for Collaboration in Security and Justice."

III.3 Removal of Indiscriminate Data Retention

The obligation for indiscriminate and mass data retention of telecommunications users' stipulated in Article 190, Section II of the Federal Telecommunications and Broadcasting Law must be eliminated, since it violates the right to privacy, as recognized by the European Court of Justice.[39]

Data retention orders must be specific and based on evidence suggesting participation in a criminal act. They should also be preceded by judicial authorization.

III.4 Clear Collaboration Methods

The regulations imposing collaboration with surveillance activities, such as Article 300 of the National Criminal Procedure Code and Article 189 of the Federal Telecommunications and Broadcasting Law, must explain the collaboration methods, and shall always require judicial authorization. The integrity and security of systems principles must be included in order to explicitly forbid surveillance capabilities that may compromise the integrity and security of communications systems.

For instance, the fact that malware is undetectable and has massive data retention capabilities compromises the right to privacy and freedom of expression. The abusive use of this type of surveillance was proven when it was revealed that authorities, like the Government of the State of Puebla (which does not have legal surveillance powers), employ

this type of malware to spy on political opponents.[40] Furthermore, there are strong indications that journalists may have also been subjected to this type of surveillance.

In these cases, the use of malware by the State, in principle, is a disproportionate measure and, consequently, it should be prohibited by law. Exceptionally, the judges must limit its use to cases in which there are no other less invasive measures to achieve the identified legitimate aim and there should be a strict, permanent judicial oversight mechanism controlling the use of this type of highly invasive surveillance technique.

III.5 Transparency

The progress made in Article 70, Section XLVII of the Federal Law for Transparency and Access to Public Information must be reflected in the Federal Law and the laws of the federative transparency organizations so that the statistical information related to surveillance is published on a regular basis on the authorities that carry out these activities websites.

Similarly, the Federal Telecommunications Institute must impose transparency obligations on telecommunications companies in the "Guidelines for Collaborations in Security and Justice," so that data about the number of requests by authorities, their type, and purpose is revealed periodically and made publicly available. It should be noted whether the requests were preceded by a judicial authority and, in such a case, whether the service provider resorts to the Judicial Branch in order to question some request made by an authority.

Moreover, transparency mechanisms related to the acquisition, purchase, import, and export of surveillance equipment and systems should be established.

III.6 Right to User Notification

The right to user notification should be included. Particularly, all laws empowering an authority to conduct mass surveillance, or any law created with that purpose, must recognize an individuals' right to be notified whenever they have been subjected to surveillance. The notification may only be delayed when the judge in charge of granting the authorization states that notifying the user may pose a risk to achieving the legitimate aim. In all cases, the law must set time limits for the delay of the notification.

This notification must include all the material obtained by the authority so that those affected may understand the content and scope of the interference and may turn to courts for redress in case of abuse.

III.7 Independent Oversight Mechanism

The law should set up an oversight mechanism for surveillance measures, or alternatively, explicit powers should be given to the oversight programs and surveillance mechanisms of the National Institute for Access to Public Information and Protection of Data (INAI), so that this authority is compelled to oversee surveillance activities. In order to do this, the Institute should be given all the material and human resources necessary, as well as the power to access all the information relevant for carrying out its duty.

This independent oversight mechanism must publish and broadly communicate the findings springing from its control obligations and it must be empowered to impose sanctions, or to file penalty proceedings for the abuse of surveillance activities.

III.8 Protection of Whistleblowers

The law must recognize immunity of individuals that, in good faith, expose a violation of the law, corruption acts, or infringements upon human rights by failing to comply with their duty of secrecy. This immunity must be explicitly recognized in the legislation imposing criminal or administrative sanctions for failing to comply with the duty of secrecy.

III.9 Effective Remedy

The Amparo Law must be interpreted by the Judicial Branch so that it recognizes the locus standi of any individual to challenge the constitutionality of the regulations that establish covert surveillance measures, without the need for the person who brings an Amparo action to prove the particular application of these regulations.

Given the secret nature of surveillance, it is impossible for individuals to detect illegitimate infringements upon their right to privacy and, thus, to judicially challenge them if an implementing act is requested.

Consequently, with a view to comply with the right to effective remedy, the legal or legitimate interest of any individual who judicially challenges these types of regulations must be recognized. For instance, the Second District Court Specialized in Telecommunications has done so in the Amparo proceedings 116/2014.[41]

1 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/text, EFF, ARTICLE19, Background and Supporting International Legal Analysis on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/AnalisisLegal, Access, Universal Implementation Guide of the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf

2 Supreme Court. Trial Chamber. Amparo in Revision 1621/2010 and Thesis Contradiction 194/2012.

3 Supreme Court. Trial Chamber. Thesis Contradiction 194/2012.

4 Supreme Court. Trial Chamber. Amparo in Revision 1621/2010 and Thesis Contradiction 194/2012.

5 Supreme Court. Trial Chamber. Amparo in Revision 1621/2010.

6 Supreme Court. Trial Chamber. Amparo in Revision 1621/2010 and Thesis Contradiction 194/2012.

7 Supreme Court. Plenary session. Complaint of Unconstitutionality 32/2012.

8 Supreme Court. Plenary session. Thesis Contradiction 293/2011.

9 Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression by the UN Special Rapporteur for the promotion and protection of the right to freedom of expression and the Special Rapporteur for the Freedom of Expression of the Inter-American Commission on Human Rights. 2013, paragraph 8.

10 ECHR. Case of Uzun vs. Germany. Application nº 35623/05. Sentence on September 2, 2010, paragraph 61; Case of Valenzuela Contreras vs. Spain. Application nº 58/1997/842/1048. Sentence on July 30, 1998, paragraph 46.

11 ECHR. Case of Uzun vs. Germany. Application nº 35623/05. Sentence on September 2, 2010, paragraph 61; Weber and Sarabia vs. Germany. Application nº 54934/00. Sentence on June 29, 2006. paragraph 93.

12 ECHR. Case of the Association for European Integration and Human Rights and Ekimdzhiev vs. Bulgaria. Application nº 62540/00. Sentence on June 28, 2007; Case of Weber and Sarabia vs. Germany. Application nº 54934/00. Sentence on June 29, 2006.

13 United Nations General Assembly. Resolution A/RES/68/167 on the right to privacy in the digital age. December 18, 2013.

14 UN. Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, Frank La Rue. April 17, 2013. A/HRC/23/40.

15 OHCHR. The right to privacy in the digital age. June 30, 2014. A/HRC/27/37.

16 IACHR. Office of the Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OEA/Ser.L/V/II.

17 Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/AnalisisLegal

18 IACHR. Office of the Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OEA/Ser.L/V/II, paragraph 165.

19 UN. General Assembly. Resolution passed by the General Assembly on December 18, 2013. 68/167. The right to privacy in the digital age. A/RES/68/167. January 21, 2014.

20 Report of the UN Special Rapporteur on the right to freedom of expression and opinion. April 17, 2013. A/HRC/23/40, available at: https://eff.org/r.z5x

21 Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression, available at: https://eff.org/r.maus

22 IACHR. Office of the Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OEA/Ser.L/V/II, available at: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

23 The Global Principles on National Security and the Right to Information, ("Tshwane Principles") drafting process culminated in Tshwane, South Africa, on June 12, 2013, available at: https://eff.org/r.flb4

24 Report of the UN Special Rapporteur on the right to freedom of expression and opinion. April 17, 2013. A/HRC/23/40

25 ECHR. Case of the Association for European Integration and Human Rights and Ekimdzhiev vs. Bulgaria. Application nº 62540/00. Sentence on June 28, 2007.

26 Animal Político. México, el principal cliente de una empresa que vende software para espiar (Mexico, main client of a company that sells spy software), available at: https://eff.org/r.4a0b

27 Animal Político / R3D. SEDENA negoció compra de software de Hacking Team en 2015 para espiar a 600 personas (Ministry of National Defense negotiates purchase of spy software from Hacking Team to spy on 600 people), available at: http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas/

28 Federal Criminal Procedure Code. Articles 278a and 278b.

29 General Law to Prevent and Punish Crimes of Abduction. Articles 24 and 25

30 Federal Law against Organized Crime. Articles 8 and 16 - 28.

31 Parliamentary Gazette of the House of Representatives. December 10, 2014.

32 Federal Police Law. Articles 48 - 55.

33 Federal Telecommunications Law. Article 44 section XII and XIII.

34 Agreement/016/2014 through which the Head of the Financial Intelligence Unit appoints the public servers mentioned herein for the purposes of the provisions established in article 189 of the Federal Telecommunications and Broadcasting Law in the Diario Oficial de la Federación (newspaper) on August 15, 2014.

35 Reuters. Mexico ramps up surveillance to fight crime, but controls lax. Available at: http://www.reuters.com/article/2015/10/12/us-mexico-surveillance-idUSKCN0S61WY20151012

36 National Security Law. Articles 33 - 49.

37 Second District Court of Administration, Specialized in Economic Competitiveness, Broadcasting and Telecommunications, based in the Federal District and with Jurisdiction throughout the Republic. Indirect Amparo 116/2014 (Carlos Alberto Brito Ocampo et al.) Sentence on February 16, 2015.

38 International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/text

39 European Court of Justice. Sentence in the cases entitled C-293/12 and C-594/12. Digital Rights Ireland and Seitlinger et al. April 8, 2014, available at: https://eff.org/r.1f5l . Press Release. The Court of Justice declares the Data Retention Directive to be invalid, available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

40 Animal Político / R3D. El Gobierno de Puebla utilizó el software de Hacking Team para espionaje político (Puebla's Government used Hacking Team Software for Political Espionage), available at: http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/

41 Second District Court of Administration, Specialized in Economic Competitiveness, Broadcasting and Telecommunications, based in the Federal District and with Jurisdiction throughout the Republic. Indirect Amparo 116/2014 (Carlos Alberto Brito Ocampo et al.) Sentence on February 16, 2015, available at: https://eff.org/r.ncyl