State Communications Surveillance and the Protection of Fundamental Rights in Mexico

By Luis Fernando García
in collaboration with Katitza Rodríguez

August 2016

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 leading a 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 an essential right both for human dignity and democracy since it allows for the exercise of fundamental rights such as freedom of expression, freedom of association, and the right to health. Nevertheless, the right to privacy is 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 for the pursue of such aims to take into consideration that these measures often threaten human rights given that they are highly invasive and tend to require secrecy in order to be effective.

The secret nature of surveillance measures poses a serious threat to individuals' dignity and the aspirations of democratic coexistence. As such, international human rights law and the constitutional doctrine of several countries have been combined to establish a set of principles that seek to inhibit abuse and guarantee accountability when it comes to modern digital surveillance.

In Mexico, although there are wide conventional and constitutional protections for the right to privacy, technical and legal capabilities for communications surveillance have been exponentially expanded within the last decade. In an institutionally-weak country like Mexico, the fact that such expansions have not been accompanied by the appropriate safeguards threatens the security of individuals, particularly of those who belong to 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 context of communications surveillance. It describes domestic regulations on this subject and 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

Article 16 of the Constitution of Mexico protects the privacy of communications. 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 the need for a federal judicial order to intercept private communications; the duty of establishing a legal basis and motivation; and clarity requirements of the petition, such as the type of interception, subjects, and duration, as well as limiting the involvement to only federal authorities appointed by law or the Public Prosecutors of state entities.

The Supreme Court in Mexico (*SCJN, in Spanish*) has interpreted this provision in the *Amparo en Revision 1621/2010* and the *Contradiction of Thesis* 194/2012. It established that the constitutional protection of private communications includes all existing forms of communication and those resulting from technological evolution such as communications made online.[2]

Likewise, the SCJN explicitly stated that the constitutional protection relative to the inviolability of communications involves 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 to protect as well the data which is external to the communication. Even though it is true that this data does not refer to the content of the communication, it is equally true that in many occasions it offers 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, habitually called 'communications traffic data,' shall be the object of analysis 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, for example, 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]

Likewise, the SCJN has recently decided that access to communications metadata stored by telecommunications companies must have prior judicial authorization.[4]

The SCJN has established that the right to privacy is violated the moment the private communication is listened to, recorded, stored, read or registered without the interlocutors' consent, regardless of the possibility of subsequent dissemination of the contents of the intercepted communication.[5]

Hence, for example, the SCJN considers an email intercepted (in such a way that it infringes upon the right to inviolability of communications) 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.[6]

The SCJN has interpreted that the constitutional protection of communications, regarding their temporal scope, 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.[7]

Notwithstanding, the SCJN has recently considered that legal obligations established in the Telecommunications and Broadcasting Federal Law that require telecommunications companies to retain communications metadata for two years, do not constitute an interference with the right to the inviolability of communication.[8]

Likewise, the SCJN has not considered that the constitutional protection given to the content of communications, as well as metadata, extends to mobile phone location data in real time. One example of this is the SCJN's decision regarding the complaint of unconstitutionality 32/2012,[9] (acciones de inconstitucionalidad in Spanish) in which the majority 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.

Thus, although at the normative level, the Constitution grants comprehensive protections for the right to inviolability of communications, the interpretation of those provisions has not been extended to protect people from mass data retention or the collection of mobile phone location data.

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 explicitly introduced the obligation of 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 articulated a doctrine that recognizes constitutional and international sources of human rights law[10] as components of the same catalog to be respected by the authority and the Mexican legal system.

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 the case of antinomy, it is understood that, in accordance with the *pro personae* principle, the most favorable norm must be preferred.

Additionally, derived from the constitutional reform of the writ of Amparo (*Acción de Amparo in Spanish*), published on June 6, 2011, the consolidation of the "parameter of constitutional consistency" (*parámetro de regularidad constitucional in Spanish*) grants the possibility of controlling the constitutionality of all regulations and acts of authorities through Amparo proceedings. In 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 developed the content and scope of the right to privacy in the context of 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 v. 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* that 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 and listening to it, as well as 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 decision confirms the adopted criteria by the Mexican Judicial Branch, in the sense that not only the content of communications is protected by the parameter of constitutional consistency, but also every other element of the communication process, that is, *metadata*, which also requires constitutional and conventional protection.

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 pointed out the importance of the adoption of the appropriate safeguards to inhibit the risks of abuse of communications surveillance measures, since they represent severe 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."*[11]

Similarly, the above-mentioned international mechanisms of protection have stated that in the context of covert surveillance activities, the law must be clear enough in its terms to provide the public with the appropriate indication about the conditions and circumstances in which authorities have the power to resort to such measures.[12]

Furthermore, in light of the risk 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.[13] Thus, in order for covert surveillance measures to comply with the *necessity test* as it applies to restrictions on the right to privacy, it is essential that there be measures mitigating 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.[14]

Accordingly, the relevance of effective guarantees against the abuse of electronic covert surveillance measures has been recently highlighted by the United Nations General Assembly (UN),[15] the UN Special Rapporteur for the Right to Freedom of Expression and Opinion,[16] the UN High Commissioner for Human Rights,[17] the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights,[18] as well as civil society organizations and experts that have gathered best practices derived from comparative case law and doctrine, and drafted the International Principles on the Application of Human Rights to Communications Surveillance.[19]

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."*[20]

The existence of independent oversight mechanisms and statistical 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 recommended 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."[21] 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. (...)"*[22]

Similarly, in the Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression,[23] 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:[24]

"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."

The Global Principles on National Security and the Right to Information, (Tshwane Principles)[25] is another document that recognizes that States are compelled to guarantee transparency with respect to surveillance programs conducted for national security purposes. Principle 10 states 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."

Another appropriate safeguard to guarantee the necessity and proportionality of surveillance measures is to notify those affected. For instance, the UN Special Rapporteur on the Right to Freedom of Expression and Opinion has recognized this right to notification:

"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."*[26]

The right to notification has also been recognized by the European Court of Human Rights, which established in the case of *Ekimdzhiev v. Bulgaria* that once the surveillance has stopped and the strictly necessary time has elapsed for the legitimate surveillance aim to no longer be at risk, those affected must be notified without delay.[27]

Thus, in international human rights law, the standards of legality, adequacy, necessity, and proportionality are enshrined and apply to 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 request the intervention of 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 Federal 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, order data retention, obtain communication devices' geolocation in real time, without judicial authorization, as well as access the metadata of communications.
	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 Kidnapping (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 for the prevention of crime, exclusively when there is a federal judicial authorization noting the existence of sufficient evidence proving that one of the crimes listed in Article 51 of this law is being carried out.
	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 of "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, through the publication of internal documents of the Italian company Hacking Team S.R.L., that a number of Mexican state and federal authorities had purchased malicious spy software,[28] most of them, without the necessary constitutional or legal powers to intercept private communications.[29]

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 prosecutors' 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.[30]

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 confirming the probable responsibility on the commission of a serious crime."

Furthermore, the CFPP stipulates that the request, and its appropriate authorization, must detail the aspects of the interception that is intended to be carried out, such as: the legal precepts on which it is based, the reasons why it is considered to proceed, 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 not prosecuted, the obtained communications must be presented before the judge and destroyed in his/her presence.

Similarly, the laws on kidnapping passed in 2010[31] and on organized crime passed in 2007[32] grant the PGR the ability to intercept private communications. The prosecution offices of each of the 31 Mexican States and of the Federal District normally 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 writing or electronic means. In other words, during an investigation of organized crime, crimes against human health, kidnapping, extortion, or other threats, the CFPP allows delivery of geographical location data of mobile communication devices in real time without judicial authorization.

The Complaint of Unconstitutionality 32/2012, filed by the National Commission on Human Rights, challenged this article. 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 the geographical location is an ephemeral measure, meaning the surveillance stops with the emergency and does not allow for sustained monitoring of 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 enter into force gradually in the several federative entities and at the federal level by June 2016 at the latest. 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 the communications, but also the data that identifies the communication—m*etadata*—either in real time or after the communicative process has taken place.

Nonetheless, the National Criminal Procedure Code (CNPP) is less clear than the Federal Criminal Procedure Code (CFPP) when referring to the appropriateness of the surveillance request only when evidence of participation exists or probable cause.

In article 303 of the CNPP, the possibility to monitor the geographical location of communication devices in real time without judicial authorization persists, and it extends to any kind of investigation, instead of to a closed list of crimes, as the CFPP establishes.

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), soon to be ruled. This ruling may generate a different precedent 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 possibility of ordering the retention of data contained in networks, computer systems or devices without a judicial order. Additionally, it does not add the necessary safeguards, such as an independent oversight mechanism,

transparency measures 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 approved a reform of Articles 291 and 303 of the CNPP firmly establishing the necessity of a federal judicial authorization to collect geographical location data, in real time, of mobile communication devices and to access data stored by telecommunications companies, Internet service providers, and application providers. This reform still requires the endorsement of the House of Representatives, which is still pending.[33]

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.[34] 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 proving the organization of [...] crimes," which are listed in Article 51 of the law.

Similarly, Article 8, section XXVIII of the aforementioned law 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 Regulation on 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 both in the case of criminal investigations, as well as for the protection of security through intelligence activities.

The Federal Telecommunications Law was amended in 2009[35] 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 12 months and applies to all users of telecommunications companies' services.

The Federal Telecommunications Law allowed the Public Prosecutor's Office and the

prosecutors of the federal entities to access data retained by telecommunications companies in order to investigate serious crimes without the necessity of obtaining a judicial authorization.

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

Article 189 of the LFTR generally establishes the obligation for telecommunications companies and online service, application, and content providers to comply with all "written requests that are well-founded and justified by the competent authority," among which "instances of security and law enforcement" are mentioned without clearly establishing which authorities fit the categories.

For example, several authorities have considered that Article 189 of the LFTR sufficiently empowers these authorities to use covert surveillance tools, and that this power does not need to be detailed in any other law. For instance, the "Financial Intelligence Unit" of the Ministry of Finance and Public Credit is considered a "security instance" pursuant to Article 189 and to an instrument that is not a formal or material law known as the "Guidelines for Collaboration" that are celebrated in the framework of National Security by the Ministry of Interior and the Ministry of Finance and Public Credit (*bases de colaboración in Spanish)*.[36] 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.[37]

Similarly, Article 190, Section I of the LFTR imposes an obligation on the concessionaires to "collaborate with the instances of security, law enforcement and administration of justice on obtaining the geographical location of the mobile communication devices in real time." This means extending the power to access "geolocation" to authorities who did not, and do not, have this power in an enabling law, such as the "security instances" or the "instances of administration of justice," which are neither defined in the LFTR nor in any other law.

Notwithstanding, the SCJN has recently established that the law must explicitly authorize authorities to carry out surveillance measures. In this way, the SCJN has clarified that the only authorities who are authorized are the Federal and State Prosecutors, the Federal Police, and the Center for Investigation and National Security (CISEN).[38]

Article 190, Section II of the LFTR requires retention of telecommunications user data. Even if this power has existed since 2009 in the now-abrogated Federal Telecommunications Law, 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) Name, business name or corporate name and address of the subscriber;*
>
> *b) Type of communication (voice transmissions, voicemail, conference, data), supplementary services (including call forwarding and transfers), or messenger or multimedia services used (including the services of short messaging, multimedia and advanced services);*
>
> *c) Data necessary to track and identify 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 necessary to determine the date, time and duration of the communication, as well as the messaging and multimedia service;*
>
> *e) Besides the previous data, 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 digital location of 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 the data for the first 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.

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 instances" is highly ambiguous, although SCJN's interpretation has reduced its understanding.

The Federal Telecommunications Institute (IFT, in Spanish), in accordance with Article 189 of the Federal Telecommunications and Broadcasting Law, has issued "Guidelines for Collaboration in Security and Justice."[39] Even though this draft does not amend the constitutional problems of the law, it recognizes some safeguards related to transparency.

In particular, Guidelines Seventeen and Eighteen establish the following:

> *SEVENTEENTH.- Without prejudice of the Telecommunications and Broadcasting Federal Law (LFTR), the Concessionaires and Authorized are responsible regarding the possession, protection, treatment and control of customers personal data. The use of stored data for different purposes from those established in the Only Chapter of the Eight Title of LFTR and these Guidelines is prohibited. Any different use will be punished by the competent authorities in accordance with the applicable law.*
>
> *EIGHTEENTH.- The concessionaires and those authorized must deliver every January and every July a semestral electronic report related to the application of these guidelines to the Federal Telecommunications Institute. This report shall contain the following:*
>
> *I. The total number by Authority, of requests for geolocation information and communications data records, breaking them down into the communications received, processed and not delivered monthly, using the format annexed to these Guidelines as Annex II.*
>
> *II. In the month of July, it must include the report referred in guideline EIGHT, section VI.*
>
> *III. In the month of January, it must include the report referred in the FORTIETH guideline.*
>
> *The Institute will request Designated or Competent Authorities to submit a semestral report in January and July of each year that is related to the number of requests for real time geographic location and communications data records, as well as the number of cancelled and erased records, once the purpose for which they were requested has been accomplished.*
>
> *In terms of what it has been established in the General Law on Transparency and Access to Public Information and other applicable provisions, the authorities referred in articles 189 and 190 of the LFTR, have the obligation to adopt all measures necessary to ensure the security of personal data and avoid its alteration, loss, transmission and unauthorized access.*
>
> *The information contained in the semestral reports shall be published on the Institute's website on the basis of the General Law on Transparency and Access to Public Information and other applicable provisions.*
>
> *In accordance with the General Law on Transparency and Access to Public Information and other applicable provisions, in the case that the systems to*

retain the data have been breached and final user personal data has been compromised, the Concessionaires and Authorized must notify the users immediately and indicate the measures that the user can take to mitigate or counter any harm produced by the breach.

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 Federal Entities Law shall stipulate that the designated subjects are compelled to make available to the public, and keep updated, in the appropriate electronic media, pursuant to their powers, attributions, duties and social objectives, accordingly, information about, at least, the following topics, documents and policies:*
>
> *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 Regulation on 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 also empowers the Center for Investigations and National Security (*CISEN, in Spanish*) to intercept private communications in the cases of "imminent threat to national security."[40] Article 5 of this law gives an extremely broad definition of the "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.

Aside from the ambiguities surrounding the circumstances under which the covert surveillance measures can be authorized, and even though both the Federal Police and the CISEN need judicial authorization to conduct these measures, laws do not establish other safeguards against abuse such as having an independent oversight body, imposing transparency obligations (requiring aggregate data of the number of surveillance requests) or requiring subsequent notification measures to the person affected by the surveillance measure.

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 reserved information as "that whose application implies 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 updating 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. It is possible to use this remedy to challenge acts or regulations infringing upon the right to privacy and the inviolability of private communications.

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 the Amparo 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, there are still some court decisions that do not acknowledge the right or capacity to bring a legal action (*legal standing or locus standi)* to challenge the regulations establishing communications surveillance measure. This happens because the plaintiff needs to demonstrate an actual (current) and real infringement by the application of the challenged regulation.

Given the secret nature of covert surveillance practices, it is practically impossible to prove the implementation of abusive surveillance measures. 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.[41]

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 twelve 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 "International Principles on the Application of Human Rights to Communications Surveillance"[42] collects and integrates the highest standards for the protection of the right to privacy in the context of State communications surveillance recognized in case law and doctrine of international human rights bodies and courts around the world.

The thirteen principles of this document are:

Legality

Any limitation to human rights must be prescribed by law. This should exist 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 and capable of fulfilling 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, actual and verifiable, to national security may be carried out. The surveillance measures used must be

the least invasive option. This means that the only information obtained, retained or used will be that which is relevant to the attainment 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 disclosure could jeopardize the achievement of the legitimate aim or an imminent risk of danger to someone's life exists.

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 develop surveillance capabilities that may compromise the security of communications and devices. Indiscriminate and massive retention of users' data must not be mandated. The right to freedom of expression must not be compromised by any obligation of identification or prohibition on 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

States should enact legislation criminalizing illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected.

IV.
Recommendations

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:

IV.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 authorization, 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 the federal judicial authorization. Particularly, the draft suggests the following addition to Article 291 (emphasis added):

> *"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 has no justification and distorts the principle of prior judicial authorization. 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, the House of Representatives should not pass this addition.

Similarly, on the subject of surveillance, Article 301 stipulates collaboration obligations that are vague and unlimited for concessionaires, licensees, and anyone in charge of media or systems susceptible of interception:

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, should 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 of the private sector 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, are not a legitimate method of collaboration between companies and the Authority.

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 of communication devices 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 kidnapping, 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 these surveillance measures may be used to investigate.

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.

IV.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 kidnapping 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 when the threat of commission of a crime or threat to national security is based on evidence that proves it is real, current and imminent. Surveillance measures must not be authorized when their aim is a general prevention.

In the case of national security, the law must establish accurately and precisely 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. 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.

IV.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.[43]

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

IV.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 clearly and precisely the collaboration methods, and shall always require judicial authorization. The Integrity and Security of Systems Principle[44] 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.[45] 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, law should generally prohibit it. Exceptionally, 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.

IV.5 Transparency

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

Similarly, the Federal Telecommunications Institute must ensure that telecommunications companies comply with the transparency obligations established in the "Guidelines for Collaborations in Security and Justice," without delay.

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

IV.6 Right to User Notification

The right to user notification should be respected and included in the national legislation. 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.

IV.7 Independent Oversight Mechanism

The law should set up an oversight mechanism for surveillance measures. 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.

IV.8 Protection of Whistleblowers

The law must recognize immunity of individuals that, in good faith, expose a violation of the law, corruption, 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.

IV.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.[46]

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. Second Chamber. Amparo in Revision 964/2015.

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

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

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

8 Supreme Court. Second Chamber. Amparo in Revision 964/2015.

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

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

11 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.

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

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

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

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

16 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.

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

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.

19 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

20 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.

21 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.

22 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

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

24 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

25 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

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

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

28 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.4aob

29 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/

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

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

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

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

34 Federal Police Law. Articles 48 - 55.

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

36 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.

37 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

38 Supreme Court. Second Chamber. Amparo in Revision 964/2015.

39 Federal Telecommunications Institute. Guidelines for Collaboration in Security and Justice. Published on the Official Gazette on December 2, 2015. Available at: http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

40 National Security Law. Articles 33 - 49.

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.

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

43 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

44 The Principle states that when compromising security for State purposes, it almost always compromises security more generally and States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users.

45 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/

46 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