Mexico

What is the legal framework that protects people's privacy in Mexico? Are my rights protected against State surveillance?

Article 16 of the Constitution protects communications privacy. Specifically, paragraphs 12 and 13 of the article specify what, according to the constitutional interpretation in Mexico, is known as the right to the inviolability of communications.

The Constitution establishes special protections against measures that may interfere with the right to the inviolability of communications. Such special protections include requiring a federal judicial authorization for the intervention of private communications, requiring the justification, legal basis, and reasoning for the intervention, and requiring clarity surrounding the type of intervention that is to be carried out—its application, targeted subjects, and duration. The power to intercept is limited to those federal authorities who are authorized by law or the Public Prosecutors of the Federal entity.

In addition, Mexico is subject to the international human rights treaties it has ratified. These treaties recognize the right to privacy and are international obligations assumed by the Mexican State and are thus applicable in domestic law.

What is the legal framework that allows for the surveillance of communications in Mexico?

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	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.

the Federal District.	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.)

Are the telecommunications companies required to retain my communications data? Under what conditions may authorities access my communications data?

The Federal Telecommunications and Broadcasting Law contains a provision that requires telecommunications companies to retain communications data (i.e. data on who communicates with whom, how often, and from what location) for a period of two years. The content of communications is excluded from this obligation.

In any case, if a competent authority needs to access the data about a user's communications or metadata, they must submit a request and obtain authorization from a federal judge. The administration of justice authorities and the federal authorities authorized by law are the only competent authorities who may submit such requests.

Is the State authorized to use malware to spy on my communications?

The legal scenario is uncertain. Authorities may claim that the same rules that exist for the interception of private communications may apply to the use of malware (i.e. it could only be employed by administration of justice authorities or federal authorities authorized by law and a federal judicial authorization would be required). However, malware is a more intrusive means of surveillance than mere communications interception. There is a need for a precise and clear legal authority that allows government officials to use malware only when there is no other less intrusive means that is equally suitable to achieving the aim.

Is my geolocation information protected under the Constitution?

Location data is partially protected in Mexico. While constitutional interpretation has considered that communications metadata is protected in the same way that communications content is protected (meaning accessing them requires judicial authorization), the Supreme Court of Justice has stated that it's not necessary to obtain judicial authorization to

monitor location data in real time.

This means that Mexican authorities must obtain a judicial authorization to access historic location data and other communications metadata stored by telecommunications companies, but they do not need authorization to monitor localization data in real time.

In encryption legal in Mexico?

Yes. There is no legislation or practice banning the use of encryption in Mexico.

How can I find out if the State is surveilling my communications?

It is very difficult to find out if the State is surveilling your communications in Mexico because there is no obligation that requires authorities to notify a person if he or she has been subject to communications surveillance.

When it comes to communications surveillance, it is necessary that the Mexican State incorporate a user notification right into its legislation. If an authority is authorized to intercept communications by law, the law must also recognize a person's right to know if they have been subjected to surveillance. Notification should only be deferred if the judge responsible for granting the authorization determines that such notification could interfere with achieving the legitimate aim. In any case, the law should set deadlines for the deferral of notification.

The notification should include a list of all of the material that was obtained by the authority during the surveillance so that the affected person can know the content and scope of the invasion of privacy and exercise their right to an effective remedy against abuse.

How many communications have been intercepted by the Mexican State?

Although no global statistics have been gathered, there have been regulatory developments that will soon provide statistical transparency for communications surveillance.

Article 70, section XLVII of the General Law of Transparency and Access to Public Information and other federal and state laws compel all authorities to publish statistics about the requests they make for communications surveillance. The statistics are supposed to include the object, scope, and legal basis for the interception and mention whether it has been carried out with judicial authorization.

Similarly, the "Guidelines for Collaboration on Security and Justice" issued by the Federal Telecommunications Institute compel telecommunications companies to issue a transparency report every six months that includes statistical information about the requests for cooperation they receive from authorities to carry out surveillance measures.

Has the Mexican State shown an interest in protecting the privacy of its citizens?

No. In July 2015 leaked internal documents from the Italian firm Hacking Team Srl. revealed that many Mexican federal and state authorities, including those in the states of Mexico, Queretaro, Puebla, Campeche, Tamaulipas, Yucatan,

Durango, and Jalisco have acquired malware and most of them do not have the constitutional[1] or legal authority to intervene on private communications.[2]

1 Political Animal. "Mexico; the main customer of a company that sells software to spy," available at: https://eff.org/r.4a0b

2 "Political Animal" / R3D. "SEDENA Negotiates Hacking Team software in 2015 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/