The State of Communication Privacy Law in Mexico

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Luis Fernando García
(R3D)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Luis Fernando García (R3D)

This report builds on the *State Communications Surveillance and the Protection of Fundamental Rights in Mexico* report, published in 2016.

EFF's Associate Director of Research, Gennie Gebhart edited this report. EFF's Engineering and Design Project Manager, Kim Carlson, along with EFF's Art Director, Hugh D' Andrade and EFF's Education & Design Lead, Soraya Okuda designed and formatted this report. EFF's engineers, Syd Young, Artemis Schatzkin, and Will Greenberg developed the revamped version of the Necessary & Proportionate website.

EFF would like to thank Luiza Rehder do Amaral, EFF Tecs-USP Fellow (2019) for her research and contributions to this report.

A publication of the Electronic Frontier Foundation, 2020.

JUNE 2020

INTRODUCTION 4

DATA PROTECTION OVERVIEW 5

1. Is there a data protection law? 5
2. Is there a data protection authority? 5
3. Does the data protection law apply to law enforcement activities? 5
4. What are the criteria, if any, for the transfer of personal data to third countries under their data protection law? 5

COMMUNICATIONS PRIVACY LAW 7

5. What's the legal authorization needed to access communications data? 7
   - Intervention of communications: judicial authorization for content and metadata 7
   - Real time location tracking and disclosure of stored data 8
6. What's the factual basis to access communications data? 8
7. Which authorities have the legal capacity to request access to communications data? 9
8. Does the country have provisions about access to data in cases of emergency? 10
9. Is there any data retention mandate? 11
10. Are there any rules that authorize the use of malware? 11
11. Is there any law that compels companies to provide direct access to their internal servers for law enforcement purposes? 12
12. Does the law compel companies to assist law enforcement agencies in their investigations? 12

TRANSPARENCY & COMMUNICATIONS PRIVACY 13

13. Does the State report on the number of requests to access communications data? 13
14. Is there any legal limitation that prohibits companies from publishing transparency reports? 13
15. Do telecommunication companies publish transparency reports? 13
16. Can companies notify users about States' data requests? 14

INTRODUCTION

This report provides condensed information on the rules for government access to communication data in criminal investigations in Mexico. It offers brief and straightforward answers on a set of relevant questions regarding when and under which conditions law enforcement authorities can gain access to users' communications data in criminal investigations as well as an overview of transparency obligations and practices.

This FAQ is intended for non-lawyers who want some general information about the legal framework for government access to data, but is not legal or technical advice.

The legal questions raised by this FAQ can be complex and the legal risks in any case will depend on the particular facts and on legal doctrines not necessarily mentioned here. This FAQ is meant to familiarize you with some of the principles involved, so that you can have a more effective discussion if and when you engage an attorney to help you with your particular circumstance.

DATA PROTECTION OVERVIEW

1. Is there a data protection law?

Yes. Mexico has adopted a federal data protection law for data held by private entities in 2010,[1] and related regulation in 2011.[2] In 2017, it adopted a data protection law for data held by public entities, which includes law enforcement agencies.[3]

2. Is there a data protection authority?

Yes. The National Institute for Transparency, Access to Information and Protection of Personal Data is the current data protection agency. Created in 2014 and renamed in 2015, it replaced the Federal Institute for Access to Information and Protection of Personal Data.

3. Does the data protection law apply to law enforcement activities?

Yes. The data protection law for data held by public entities includes law enforcement activities.[4] It defines public entities as any authority, entity, or body of the Executive, Legislative or Judicial Powers, autonomous units, political parties, trusts, public funds, or Unions. It also includes any other natural or legal person who receives and exercises public resources or performs acts of authority at the federal, state, or municipal levels.[5]

4. What are the criteria, if any, for the transfer of personal data to third countries under their data protection law?

If the data controller transfers personal data to third-party nationals or foreigners (other than the data controller), it should communicate the transfer in the privacy notice including the purposes of the transfer. The data should be processed according to the privacy notice, and should contain a clause indicating whether the data subject consents or not to the transfer. Likewise, the third-party recipient will agree to assume

[1] Federal personal data protection law held by private sector (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), available at http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (Spanish)
[2] Regulation of the federal personal data protection law held by private sector (*Regulacion de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf (Spanish)
[3] Comprehensive law for the protection of personal data held by public entities (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), available at http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf (Spanish)
[4] Comprehensive law for the protection of personal data held by public entities (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), available at http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf (Spanish)
[5] Article 1 of the comprehensive law for the protection of personal data held by public entities. http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017 (Spanish)

the same obligations that correspond to the person responsible for transferring the data. [6] The transfers of personal data to third-party nationals or foreigners can be done without consent in specific cases specified in the law, such as if the transfer is established in a law or Treaty that Mexico is part of, if the transfer is needed for medical or sanitary treatment, or if the transfer is needed or legally obligatory for the protection of the public interest, among others.[7]

[6] Article 36 of the Federal personal data protection law held by the private sector. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (Spanish)
[7] Article 36 of the Federal personal data protection law held by the private sector, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (Spanish)

COMMUNICATIONS PRIVACY LAW

5. What's the legal authorization needed to access communications data?

The Mexican Constitution protects the privacy of communications and personal data.[8] Every person has the right to enjoy protection on their personal data, and to access, correct, and delete such data. All people have the right to oppose the disclosure of their data, according to the law.

Intervention of communications: judicial authorization for content and metadata

Article 16 of the Mexican Constitution requires that any intervention of any private communication be authorized by a federal judicial authority exclusively and upon the request of the federal authority appointed by law, or by the public official of the Attorneys' General Office of the federal entity. The competent authority shall establish and justify the legal reasons for the request, specifying the type of interception, its subjects, and its duration. The federal judicial authority must not grant these authorizations in electoral, tax, commercial, civil, occupational, or administrative cases, nor in cases of communications between the accused and his/her attorney.[9]

Article 252 of the National Criminal Procedural Code requires prior authorization from the judge (*Juez de Control*) for any investigation that will impact any rights established in the Mexican Constitution. Article 291 established that the Head of the Office of the Attorney General (including those to whom they delegate this authority, and their counterparts in each federal entity) may request authorization from the competent judicial authority to intercept communications when the Public Prosecutor deems it necessary.[10] The intervention of private communications, as defined by the statue, covers all communication systems, or programs that are the result of technological evolution, and that allow the exchange of data such as information, audio, video, and messages, as well as electronic files that record and retain the content of the conversations or data that identifies the communication, all of which can be presented in real time.[11]

Judicial authorization will also be required in cases of information extraction, which consists of obtaining private communications or identification data of the

[8] Constitution of Mexico, article 16, (12), http://www.sct.gob.mx/JURE/doc/cpeum.pdf. Article 16, paragraphs 12 and 13.
[9] National Code for Criminal Procedure, article 294, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)
[10] National Code for Criminal Procedure, article 291, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)
[11] National Code for Criminal Procedure, article 291, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)

communications, as well as data, documents, text, audio, image, or video files contained in any device, computer equipment, or storage device that may contain data, including those stored on platforms or data centers that are remotely linked to these devices.[12]

Real time location tracking and disclosure of stored data

Article 303 of the National Criminal Procedure Code states that the Head Attorney General or those to whom they delegate this authority can request the competent judicial authority to order telecom companies, and content and application providers of the mobile devices associated with a mobile line that is under criminal investigation, to disclose location data in real time or to disclose retained metadata in a timely and sufficient way when the Public Prosecutor deems it necessary. Data should be destroyed if it is not relevant for the criminal investigation.[13]

6. What's the factual basis to access communications data?

The National Criminal Procedure Code established that the request for intervention must: specify the person or persons who will be subject to the measure; identify the place or places where it will be held, if possible; the type of communication to be intervened; its duration; the process of intervention that will be carried out and the lines, numbers, or devices that will be intervened; and, where appropriate, the name of the telecom company through which the communication is carried out, as well as the period during which the intervention will be conducted (which must not exceed six months).[14] The judge must verify compliance with the terms of authorization, and in case of non-compliance the judge must decree its partial or total repeal.[15]

The National Guard Law empowers the National Guard to intercept private communications to prevent certain crimes established by law.[16] The law explicitly states that the judicial authorization for the intervention of private communications shall be granted "only upon the request of the Commander or the Head of the General Headquarters of Police Coordination (*titular de la Jefatura General de Coordinación Policial*), when there is sufficient evidence proving the organization of [...] crimes".[17] The authorities responsible for carrying out the interventions must be governed by the principles of legality, objectivity, efficiency, professionalism, impartiality, honesty, and respect for human rights provided for in the Constitution.[18] The National Guard must also render a report on the intervention that the competent judge authorizes to the

[12] National Code for Criminal Procedure, article 291, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)
[13] National Code for Criminal Procedure, article 303, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)
[14] National Code for Criminal Procedure, article 292, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)
[15] National Criminal Procedure Code, Article 294 http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)
[16] National Guard Law, Article 100 and 103, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)
[17] National Guard Law. Articles 100 and 103, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)
[18] National Guard Law. Articles 101, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)

Public Ministry.[19] Finally, only the National Guard staffers who meet the following requirements can comply with the prior judicial authorized interventions: those national guard staff who are part of the investigative entities or specialized technical services; who have obtained a valid certification of trust; and have a minimum degree of sub-inspector.

The National Guard can also request, with prior judicial authorization, any type of information, including mobile location data in real time from the service providers and operators of telephone or satellite services and from all telecommunications companies in order to prevent a crime. The competent judicial authority must resolve the request within a period not exceeding twelve hours from its presentation.[20]

The National Guard Law[21] empowers the Centro Nacional de Inteligencia (CNI) to intercept private communications in the cases of "imminent threat to national security".[22] The law also gives an extremely broad definition of the "threats to national security."[23] Furthermore, the law restricts access to information with respect to national security in a broad and vague manner.[24]

7. Which authorities have the legal capacity to request access to communications data?

Article 16 of the Mexican Constitution exclusively provides that the federal judicial authority, at the request of the competent federal authority prescribed by law or the Head of the Federal Public Ministry, may authorize the intervention of any private communication.

According to Mexican Federal Legislation, the following authorities are the only ones authorized to request such intervention:

[19] National Guard Law. Article 104, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)
[20] National Guard Law. Article 9, section XXVI, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)
[21] National Guard Law, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)
[22] National Guard Law, Articles 33 - 49, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)
[23] 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.
[24] 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."

- The Head of the Office of the Attorney General (*Fiscalía General de la República*), including those to whom they delegate this faculty, and their counterparts in each of the federal entities[25]
- The Commander of the National Guard or the Head of the General Headquarters of Police Coordination[26]
- National Intelligence Center - CNI (Executive Branch)[27]

In terms of national security, the National Security Law authorizes the National Intelligence Center - CNI to intercept private communications if an "imminent threat to national security" exists.[28] "Threats to national security" are broadly defined in Article 5 of the National Security Law. For example, actions aimed at carrying out espionage, sabotage, terrorism, revolt, treason, or genocide against the United Mexican States within its national territory; actions of foreign interference with national issues that may have a negative impact on the Mexican State; actions disabling authorities to take action against organized crime; actions aimed at hindering or obstructing intelligence or counterintelligence activities' and actions aimed at destroying or disabling the strategic or needed infrastructure for the provision of public goods and services, among others.

8. Does the country have provisions about access to data in cases of emergency?

Article 303 of the National Procedure Code states that in exceptional cases, when the physical integrity or life of a person is in danger or the victim of the crime is at risk, and when the facts investigated are related to the illegal deprivation of liberty, kidnapping, extortion, or organized crime, the Attorney General, or the public servant to whom this faculty is delegated, under the strictest responsibility, can directly request access to location data in real time or the disclosure of retained data stored by telecom companies or content or application providers. Those companies are obliged to act immediately. Once the request has been fulfilled, the Public Ministry must inform the competent judge (*Juez de Control*) within 48 hours so the judge can ratify the emergency measure in full or partially, notwithstanding that the Public Ministry will continue with their action. If the judge does not ratify the emergency intervention measure, the information obtained can not be incorporated in the criminal procedure.

The Guidelines for Collaboration on Security and Justice Matters[29] and the Federal Telecommunications Act[30] set out that the providers must implement the necessary

[25] National Code for Criminal Procedure, article 291, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf (Spanish)
[26] National Code for Criminal Procedure, article 100, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGN_270519.pdf (Spanish)
[27] According to National Security Law (Articles 33 – 49) and Federal Telecommunications and Broadcasting Law (Articles 189 – 190). See also article 30 Bis XVII, http://www.diputados.gob.mx/LeyesBiblio/pdf/153_220120.pdf
[28] Mexico, National Security Law. Articles 33 - 49.
[29] Guidelines for Collaboration on Security and Justice Matters. http://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/dofpiftext111115159.pdf (Spanish). Section 7.
[30] Federal Telecommunications Act. Article 190, IX.

measures for enabling access to location data in real time or retained data in cases of emergency.

9. Is there any data retention mandate?

Article 190 of the Federal Telecommunications and Broadcasting Act (LFTR) of 2014 orders telecommunications providers to retain data for 12 months on systems that allow law enforcement agencies to access and obtain the data electronically, in real time. After this one-year period, telecommunications providers must keep the data for an additional 12 months and, upon request, deliver it to authorities within 48 hours.[31] The Mexican Supreme Court recently declared this law constitutional, stating that this data retention obligation does not constitute an interference with the right to the inviolability of communications.[32]

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

- Name, business name, or corporate name and address of the subscriber
- 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)
- Data necessary to track and identify the origin and destination of mobile communications: destination number, types of line service (i.e. lines with a contract or a flat rate plan, like the lines of prepaid credit)
- Data necessary to determine the date, time, and duration of the communication, as well as the messaging and multimedia service
- Besides the previous data, the date and time of the first service activation and localization tag (Cell ID)
- When appropriate, the identification and technical characteristics of the device, including, among others, the international ID codes of the subscriber and the make and model of the device
- The digital location of the geographical position of the lines

The obligation to store data shall begin since the date on which the communication is produced.

10. Are there any rules that authorize the use of malware?

In Mexico, there is no specific law that regulates the use of malware. However, the legislation recognizes the possibility that some authorities may require federal judicial authorization for the intervention of private communications for specific purposes, and that might be the legal authority used by the Mexican Government. Those authorities

[31] Federal Telecommunications and Broadcasting Law.
http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014 (Spanish)
[32] Second Chamber, Supreme Court, Amparo in Revision 964/2015.

are: Office of the Attorney General of the Republic and Offices of the states of the Federation, National Intelligence Center (CNI), and National Guard.[33]

11. Is there any law that compels companies to provide direct access to their internal servers for law enforcement purposes?

To the best of our knowledge, there is no legal provision authorizing this kind of direct or remote access to servers in criminal investigations. Article 189 of the Telecom Law authorizes telecom, content and application providers to comply with the competent authority's access request in the terms established by law.

12. Does the law compel companies to assist law enforcement agencies in their investigations?

Article 301 of the National Criminal Procedure Code sets out that telecom and Internet providers, and any other company that can intervene in a private communication, shall be compelled to collaborate with the authorities in such measures when requested and in an efficient manner. Likewise, such companies must have the necessary technical capacity to meet the requirements requested by the judicial authority to comply with a communications intervention order.[34]

[33] R3d.mx, Article 19, Social Tic, Gobierno Espia, Vigilancia sistematica a periodistas y defensores de derechos humanos en Mexico https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf (Spanish)
[34] National Criminal Procedure Code, Article 301.

TRANSPARENCY & COMMUNICATIONS PRIVACY

13. Does the State report on the number of requests to access communications data?

Yes. In Mexico, governmental agencies must regularly disclose statistical information about the requests they have made to telecommunications service providers for communication interceptions, access to communications records, and access to location data in real time. Article 70 of the 2015 Transparency Law established that the government should make available to the public, and keep updated, data, among others, 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."

14. Is there any legal limitation that prohibits companies from publishing transparency reports?

No, to the contrary. Mexico had an obligation compelling companies to publish transparency reports, which was repealed. The Federal Telecommunications Institute (IFT, in Spanish), in accordance with Article 189 of the Federal Telecommunications and Broadcasting Law, issued a guideline that regulated the collaboration between the government and the private sector. The guideline required telecom companies to submit transparency reports regarding the number of users' data requests to the Telecommunications Federal Institute every six months,[35] which was repealed by the Mexican Telecom regulator, IFT.

15. Do telecommunication companies publish transparency reports?

- AT&T publishes regular transparency reports. Although the report provides very little data for most of the Latin American and European countries, it is more detailed in Mexico's section. Regardless, it is still not as detailed as the report for the U.S. .

- Telefónica - Movistar publishes yearly transparency reports.

[35] Guidelines for Collaboration in Security and Justice. December 2, 2015. http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015 40. National Security Law. Articles 33 - 49.

- Telmex/Telcel does not disclose transparency reports.
- Axtel does not disclose transparency reports.
- Megacable does not disclose transparency reports.
- Izzi does not disclose transparency reports.
- Totalplay does not disclose transparency reports.

16. Can companies notify users about States' data requests?

There is no legal provision that establishes a mandatory obligation to notify the user that their data was requested by the State.