Information on Legal Frameworks in Mexico Pertaining to Privacy and Freedom of Expression

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

1.1 Political Constitution of the United Mexican States

Under Article 16 of the Constitution, no person shall have their private affairs, or home invaded, without a written order from a competent authority.

In the constitutional proceedings of *Amparo en Revision* 1621/2010 and *Contradiction of Thesis* 194/2012 the Supreme Court of Mexico confirmed that the constitutional protection of private communications extends to all existing forms of communication, including communications made over the internet.

Only the federal judicial authority can authorise interception of private communications, either at the request of the appropriate federal authority or of the State Public Prosecution Service. The authority that makes the application must present in writing the legal case for the request and set out the type of interception required, the individuals to be subjected to the interception and the proposed duration of the interception.

The federal judicial authority cannot authorise interception of communications in cases relating to electoral, fiscal, commercial, civil, labour or administrative matters or attorney-client communications relating to criminal matters.

Authorised interceptions of communications are subject to the requirements and limitations set out in the law. The results of interception of communications that do not comply with such requirements cannot be admitted as evidence in judicial proceedings.

1.2 National Code of Criminal Procedures ("NCCP")

Article 291 of the NCCP states that when they consider that interception of private communications is required to investigate a crime under the National Criminal Code, the Attorney General, or the appropriate Units within its office, or federal or local prosecutors may submit a request to a federal judge to initiate the interception of communications.

The authorisation issued by the federal judge to intercept private communications may apply to any communication system, or software which allows for the exchange of data, information, audio, video, messages or to electronic files that record the contents of conversations, or to information identifying communications that can be provided in real-time.

Interception requests must be considered immediately by a judge and, in any event, must be decided within six hours. The interception must be carried out by a means which ensures the fidelity of the evidence collected or under the supervision of the Public Prosecutor.

Interception requests must set out the legal basis and reasons for the application. They must include the:

(a) name of individuals to whom they apply;

(b) place where the interception is to take place;

(c) period of interception;

(d) procedure to be implemented (including the phone lines, numbers or devices that will be intercepted);

(e) name of the telecommunications company through which communication is routed; and

(f) the type of communications that will be intercepted if possible (Article 292).

The judicial authorisation must set out the terms and conditions for the interception (Article 293). The period of interception may not exceed six months, including any extensions. After this period, interceptions may only be authorised if the relevant Public Ministry submits new arguments justifying such extension.

All intercepted communications must be stored in a way which does not affect their fidelity, authenticity and content in order for them to be admissible as evidence. Evidence must be destroyed at the end of investigation if it is not to be used in court or if the trial is resolved or dismissed or if the defendant is acquitted.

Article 301 requires that all concessionaries, authorised telecommunications service providers and owners of communication systems which may be intercepted (including private networks) ("**CSPs**") cooperate with the authorities and have the technical capacity to implement authorised interception measures. CSPs must therefore implement interception orders they receive on behalf of the requesting authority.

At the conclusion of the investigation, the Public Prosecutor must review the results and provide the competent judge with a summary report.

1.3 **Federal Law Against the Organized Crime ("*Ley Federal Contra la Delincuencia Organizada*" - "LAOC")**

Articles 1 and 27 LAOC specifically state that interception of private communications can be carried out in order to investigate crimes in which it is assumed on good grounds that organized crime is involved. CSPs must cooperate with the authorities in accordance with the relevant judicial order for these purposes.

1.4 **General Law to Prevent and Sanction Kidnapping Crimes ("*Ley General Para Prevenir y Sancionar los Delitos en Materia de Secuestro, Reglamentaria de la Fracción XXI del Artículo 73 de la Constitución Política De Los Estados Unidos Mexicanos*" - "LPSKC")**

Under Article 24 LPSKC, interception of communications for the purposes of investigating kidnapping offences must also comply with the NCCP.

1.5 **Federal Police Law ("*Ley de la Policia Federal*" – "FPL")**

Article 48 FPL states that judicial authorisation for interception of communications by federal police must be requested by the General Commissioner where there is evidence of certain specified offences (set out in Article 51). Such interception must also comply with the NCCP and the Constitution.

1.6 **Federal Telecommunications and Broadcasting Law ("*Ley Federal de Telecomunicaciones y Radiodifusión*" - "FTBL")**

According to articles 189 and 190 of the FTBL, concessionaires and, where appropriate, authorised entities, and service providers providing communication software applications are required to allow the corresponding competent authorities to intercept private communications and provide the support requested in accordance with the law.

The term "competent authorities" is not defined in the legislation. However, in the Amparo Review 964/2015 the Mexican Supreme Court held that the competent authorities are the Federal and State Prosecutors, the Federal Police, and the Center for Investigation and National Security. While this resolution is not binding, it will be pertinent to the interpretation of Article 189 FTBL in the future.

The FTBL does not provide for revocation of a concession for not complying with Articles 189 and 190 of the FTBL. However, failure to comply with such obligations would incur a fine equal to between 1.1% and 4% of revenue (Article 298). Furthermore, under Article 178 Bis of the Federal Criminal Code individuals to whom FTBL applies or certain persons authorised to represent a CSP may be sentenced to three to eight years in prison and a fine equal to 5,000 to 10,000 times the daily general minimum wage.

1.7 **Guidelines for Collaboration on Security and Justice (*"Lineamientos de Colaboración en Materia de Seguridad y Justicia"* - "Guidelines")**

The Guidelines issued by the Institute of Federal Telecommunications ("**IFT**") provide further information in relation to Articles 189 and 190 of the FTBL. This includes practical guidance such as the format in which communications data should be provided when requested.

1.8 **State legislation**

In addition to the federal legislation discussed above, there are also state laws under which interception of communications can be approved through an application by the Public Prosecutor of the relevant state to a federal judge.

2. DISCLOSURE OF COMMUNICATIONS DATA

Under article 190(II) FTBL, CSPs are required to keep records of communications accurately identifying the:

(i) name of the subscriber;

(ii) type of communication (such as voice, voicemail, conferencing or data), supplementary services, messaging or multimedia services;

(iii) data necessary to trace and identify the source and destination of mobile communications (such as number and tariff plan);

(iv) data necessary to identify the date, time and duration of a communication;

(v) date of initial activation of the service provided and the cell site;

(vi) identification and technical characteristics of the devices (including the IMEI and IMSI); and

(vii) the digital geographical positioning location of telephone lines (in real time).

Article 190 (III) FTBL, requires CSPs to provide such records on request from the relevant authorities. Under paragraph 3 of the Guidelines, these records should be kept for a minimum of 24 months.

Under Article 303 NCCP, when the Public Prosecutor's Office deems that real-time geographical location data or delivery of the data retained by CSPs is required, the Public Prosecutor, or its authorised representative, may apply for a judicial order requesting this from the relevant CSP.

The request must set out the relevant mobile communication equipment, the facts supporting the need for real-time geo-location or data, the time period for which it is required and the name of the company or supplier of the communications service through which the lines, numbers or devices that will be the object of the measure are operated.

The request must be considered and decided by the judicial authority immediately and must be carried out by a means which ensures the fidelity of the evidence collected or under the supervision of the Public Prosecutor.

If the judge denies the application, the Public Prosecutor's Office may remedy the deficiencies in the application and reapply or may appeal the decision. Under Article 467 of the Federal Criminal Code, a refusal to grant the order could be challenged through an appellate procedure before a Federal Higher Court of three magistrates. The appeal must be resolved within twelve hours.

In exceptional circumstances such as when the safety of a person or the successful investigation of a crime is at risk or in cases of kidnapping or organised crime the Public Prosecutor may request communications or geo-location data from CSPs without a court order. In such cases the request must be notified to and retrospectively ratified by a judge within 48 hours in order for the information obtained to be admissible as evidence in criminal proceedings.

The Public Prosecutor may also require CSPs to preserve any data contained in networks, systems or computer equipment for up to 90 days.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 National Security Law ("*Ley de Seguridad Nacional*" - "NSL")

Articles 33 to 36 of the NSL establish that in case of an immediate threat to national security, the Mexican Government (through the Attorney General) can request a judicial warrant to intercept private communications to protect national security.

In addition to Articles 189 and 190 FTBL, Article 46 NSL requires CSPs to allow the competent authorities to intercept private communications and to provide the support that such authorities request in accordance with the law.

For the purposes of the NSL, the following are considered threats to national security:

(i) acts aimed at committing espionage, sabotage, terrorism, rebellion, treason or 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 Mexican 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 and of chemical, biological and conventional weapons of mass destruction;

(ix) unlawful acts against maritime navigation;

(x) any act involving the financing of terrorist acts and organisations;

(xi) acts aimed at obstructing or blocking espionage or counterespionage activities; and

(xii) acts aimed at destroying or disabling strategic infrastructure or infrastructure essential for the provision of goods or public services.

Under Article 38, the Director of the Centre for Investigation and National Security ("**CISEN**") (acting through the Attorney General) must make a reasoned application setting out a thorough description of the facts which constitute a threat to national security. The application must not contain information which identifies people, places or affairs where undue disclosure might jeopardise their safety or an investigation. However, such information must be submitted to the judge in a sealed envelope attached to the application and stored in the court safe.

In the order authorising the interception, the judge must set out the information sought, the type of activity authorised, the term of the authorisation, express authorisation to install or remove any instrument or means for the interception required and anything else the judge considers necessary (Article 40).

Under Article 43, interceptions may be authorised for up to 180 days. In exceptional circumstances, the judge may authorise an extension of up to a period equal to the original authorisation.

The judge must make the order within 24 hours of receipt. However, in cases of emergency in which following the procedures set out in Articles 37 to 42 would jeopardise the successful outcome of an investigation and threaten national security, the judge may authorise the required measures immediately (Article 49).

Interceptions are executed by CISEN with the cooperation of CSPs. The judge may request periodic updates regarding the execution of the order to ensure that its terms are being complied with (Article 41).

3.2 Guidelines

According to the Guidelines, when a government agency requires access to customers' information, CSPs should prioritise cases involving national security or where the life of a person is threatened.

3.3 Political Constitution of the United Mexican States

In cases of invasion, serious breach of the peace or any other event which may place society in severe danger or conflict, the President can suspend constitutional rights and guarantees which may constitute obstacles to rapidly and effectively resolving the situation (Article 29). This may include prohibition on interception of private communications in Article 16 of the Constitution and may apply throughout the country or in specified regions.

Restriction or suspension of constitutional rights or guarantees must:

(a) be based on the provisions established by the Mexican Constitution;

(b) be proportional to the danger; and

(c) observe the principles of legality, rationality, notification, publicity and non-discrimination.

In order to implement such a restriction or suspension of constitutional rights, the President (as the Executive Power) must consult all Secretaries of State and the Attorney General, and must obtain Congressional approval.

Suspensions of constitutional rights and guarantees must be temporary and general (a suspension can never be applied on a single person). If suspension is requested during the Congressional recess, Congress will be reconvened immediately and will then grant the authorisations necessary to deal with the situation.

3.4 FTBL

Under Article 117 FTBL, in cases of natural disaster, war, imminent danger to national security, the country's interior peace or the national economy or in order to guarantee the continuity of the public services, the Federal Executive, through the Ministry of Communications and Transportation, may requisition general means of communications (including networks), as well as the movable and immovable properties necessary to operate said means and use them as it deems appropriate. In such a situation, the IFT must provide the necessary technical support.

The personnel working for the CSP may be used to assist if this is deemed appropriate and any such requisition may continue for as long as the underlying cause remains.

Under Article 117, other than in cases of war the Federal Executive must indemnify the interested parties for losses caused by the requisition. If the value of such losses

cannot be agreed, they must be calculated by a jointly appointed expert (based on the average net income of the indemnified party for the year prior to the requisition). The expert's costs are split equally between the parties.

The affected party may also file a constitutional appeal against the requisition and/or the level of indemnification.

4. CENSORSHIP-RELATED POWERS

4.1 FTBL

According to Article 190(VII) FTBL and the Guidelines, the competent authorities can request that a federal judge immediately suspend the mobile telephone service (and/or other subscription services) in order to bring an end to the commission of criminal offences in accordance with applicable laws (or in case of theft or loss of the mobile device or duplication of the IMEI).

The IFT has overall responsibility for overseeing compliance with FTBL.

There are no regulations which specifically require CSPs to block IP addresses or ranges of IP addresses. However, the FTBL promotes net neutrality and in accordance with Articles 145 and 146, concessionaries and authorised internet service providers must comply with general principles promoting:

(i) free choice;

(ii) non-discrimination;

(iii) privacy;

(iv) transparency and information;

(v) traffic administration;

(vi) quality; and

(vii) sustained development of infrastructure.

In the future the IFT may issue further guidelines regulating the net neutrality principles which may cover the possibility of blocking websites or IP addresses and/or ranges of IP addresses but these have not yet been published.

4.2 Mexican Constitution

It is possible that federal judges could order the blocking of IP addresses or ranges of IP addresses through the use of general powers under Article 16 to implement measures assuring due compliance with the relevant laws. However, there are no specific provisions which provide for orders blocking websites or IP addresses.

5. Guidelines for Cooperation between Penitentiary Authorities and Concessionaires of Telecommunications Services and Technical Rules for the Installation and Operation Inhibition Systems ("Lineamientos de Colaboración entre Autoridades Penitenciarias y los Concesionarios de Servicios de

Telecomunicaciones y Bases Técnicas para la Instalación y Operación de Sistemas de Inhibición" – "Penitentiary Guidelines")

The Penitentiary Guidelines state that all federal, state and local jails, prisons, penitentiaries and similar centres must have equipment to permanently block or cancel mobile telephony, radio-communications and the transmission of data or images within their perimeters.

Under Article 16, CSPs must collaborate with the competent authorities to establish the necessary mechanisms to prevent and, if necessary, resolve any undue use of telecommunications services in such locations.

The Ministry of Public Security has overall responsibility for ensuring compliance with the Penitentiary Guidelines.

6. PUBLICATION OF LAWS AND AGGREGATE DATA RELATING TO LAWFUL INTERCEPT AND COMMUNICATIONS DATA REQUESTS

6.1 Publication of laws

There are no restrictions on the publication of laws in Mexico.

6.2 Publication of aggregate data

(a) **The General Law on Transparency and Public Information Access ("Ley General de Transparencia y Acceso a la Información Pública")**

(b) Article 70(XLVII) states that the relevant authorities must maintain a list of requests made to CSPs related to interception of private communications, the access to communication data and real-time geo-location of communication equipment for statistical purposes. These records must include the object and term of the measures, the legal provisions on which the requests were based and whether a judicial authorisation was granted.

(c) **Guidelines for Collaboration on Security and Justice (*"Lineamientos de Colaboración en Materia de Seguridad y Justicia"* - "Guidelines")**

Paragraph 17 of the Guidelines states that the personal data retained by CSPs can only be used for the purposes of the Guidelines. CSPs must provide information about interception and data requests from authorities to the IFT who then publish statistical information in its website on a biannual basis.

Transparency reports and statistics may be published by CSPs provided that they do not contain any personal data or information that may identify an individual.

Law stated as of 28 October 2016.