PRIVACY INTERNATIONAL

The Right to Privacy in Mexico

Stakeholder Report Universal Periodic Review 17th Session - Mexico

Submitted by Privacy International March 2013

The Right to Privacy in Mexico

Stakeholder Report
Universal Periodic Review
17th Session - Mexico

Submitted by Privacy International
March 2013

Privacy International 46 Bedford Row, London, WC1R 4LR, GB

Introduction

This stakeholder report is submitted jointly by Privacy International (PI), a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.[1] PI wishes to bring concerns about the protection and promotion of the right to privacy in Mexico before the Human Rights Council for consideration in Mexico's upcoming review.

The right to privacy

Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[2] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, ad "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[3] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[4]

As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate a number of State obligations related to the protection of personal data.[5] A number of international instruments enshrine data protection principles,[6] and many

---

[1] PI is also grateful to Hiram Piña, law school researcher at the Autonomous University of Mexico State, for his input.

[2] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[3] Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[4] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[5] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[6] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

domestic legislatures have incorporated such principles into national law. Data protection is also emerging as a distinct human or fundamental right: numerous countries in Latin America and Europe have now recognised data protection as a constitutional right, and the recently adopted ASEAN Human Rights Declaration explicitly applies the right to privacy to personal data (Article 21).

Follow up with the previous UPR

The previous UPR of Mexico took place on 10th February 2009. The Working Group report[7] made no explicit mention of the right to privacy. On the other hand, there were widespread concerns about the suppression of press freedom, and violence against journalists, with several relevant recommendations including "inviting NGOs working on press freedom to a constructive dialogue on how Mexico can ensure press freedom", "undertaking legal reforms to ensure openness and transparency of the media in the country, reviewing legislation governing radio, television and communications, and following up on the Supreme Court's ruling for a new legal framework permitting diversity in the media."[8] Mexico's National Report for the UPR in 2009 did not directly address the issue of the right to privacy, but did mention the subject of access to public information and the Federal Institute for Access to Information as the body whose responsibility it is to promote the exercise of the right of access to information and to protect personal data kept by executive branch agencies and institutions.[9]

Mexico's National Program for Human Rights 2008-2012[10] makes no explicit mention of the right to privacy.

At the time of the last UPR Mexico was formulating its new data protection law, the Federal Law for the Protection of Personal Data in Control of Private Persons (see below), and an amendment concerning data protection to Article 16 of its Constitution (see below).

Domestic laws and regulations related to privacy

Article 16 of the Mexican Constitution of 1917 provides extensively for the right to privacy, including protection of the person, his/her family, documents or possessions, and the confidentiality of correspondence. An additional paragraph was added in June 2009 which provides for the protection of personal data. This is a new constitutional guarantee that recognises the rights of citizens to access, correct, cancel or oppose the management of their personal data. Article 16 provides, in part:

> "An individual's person, family, home, papers or possessions may not be invaded without a written order from a competent authority, duly explaining the legal cause of the proceeding.

---

[7] Report of the Working Group on the Universal Periodic Review, Mexico, 29 May 2009, available at: http://www.unhcr.org/refworld/topic,459d17822,485683562,49f964f20,0,,,MEX.html

[8] Ibid.

[9] Ibid.

[10] Mexico's National Program for Human Rights 2008-2012, published on 29 August 2008, available at: http://www.ohchr.org/Documents/Issues/Education/Training/actions-plans/Mexico1.pdf

Everyone has the right to enjoy protection of their personal data, and to access, correct and cancel such data. Everyone has the right to oppose disclosure of his data, according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of third party's rights.

[…]

Only a judicial authority can issue a search warrant at the request of the Public Prosecution Service. The search warrant must describe the place to be searched, the person or persons to be apprehended and the objects to be seized. Upon the conclusion of the search, a report must be compiled at the site in the presence of two witnesses proposed by the occupant of the place searched or, in his absence or refusal, by the acting authority.

Private communications shall not be breached. The law shall punish any action against the liberty and privacy of such communications, except when they are voluntarily given by one of the individuals involved in them. A judge shall assess the implications of such communications, provided they contain information related to the perpetration of a crime. Communications that violate confidentiality established by law shall not be admitted in any case.

Only the federal judicial authority can authorize telephone tapping and interception of private communications, at the request of the appropriate federal authority or the State Public Prosecution Service. The authority that makes the request shall present in writing the legal causes for the request, describing therein the kind of interception required, the individuals subjected to interception and the term thereof. The federal judicial authority cannot authorize telephone tapping nor interception of communications in the following cases: a) when the matters involved are of electoral, fiscal, commercial, civil, labor or administrative nature, b) communications between a defendant and his attorney.

The judiciaries shall have control of judges who shall immediately and by any means solve the precautionary measures requests and investigation techniques, ensuring compliance with the rights of the accused and the victims. An authentic registry of all the communications between judges and the Public Prosecution Service and other competent authorities shall be kept.

Authorized telephone tapping and interception of communications shall be subjected to the requirements and limitations set forth in the law. The results of telephone tapping and interception of communications that do not comply with the aforesaid requirements will not be admitted as evidence.

Administrative authorities shall have powers to search private households only in order to enforce sanitary and police regulations. Administrative authorities can require accounts books and documents to corroborate compliance with fiscal provisions, following the procedures and formalities established for search

warrants. Sealed correspondence circulating through the mail shall be exempt from any search and the violation thereof shall be punishable by the law."[11]

Article 73, XXIX-O of the Constitution grants Congress the power to protect, and regulate the use of, personal data held by private entities.[12]

Articles 210, 211 and 211 Bis of the **Mexican Penal Code (Código Penal Federalo)**[13] specify sanctions ranging from six to 12 years of imprisonment and fines of 300 to 600 days of salary for those who reveal, disclose, or unduly use to the detriment of others, information or images obtained during the interception of a private communication. **Articles 211 Bis 1 – 4**[14] address the issue of cybercrime and provide substantial penalties for individuals who modify, copy, destroy, or cause loss of information contained in secure computer systems and equipment (including governmental and financial computer systems and equipment). **Article 214** protects the disclosure of personal information held by government agencies.

The **Federal Transparency and Access to Public Government Information Law**[15] (**LFTAIPG** is the law's Spanish acronym) regulates the right of everyone to access information held by government bodies and sets forth the criteria, procedures and principles by which the right of access before federal authorities can be enforced. The law standardises principles under which the various organs of the State must process citizens' personal data, including consent and purpose specification principles, and guarantees of rights of access and correction. The LFTAIPG provides that all government information is public and instructs government authorities to uphold and promote the "principle of maximum disclosure and availability of information," which means that in case of doubt as to whether the information is public or private in nature, it should be resolved in favour of the right of access thereto.

A new data protection law, the **Federal Law for the Protection of Personal Data in Control of Private Persons**[16] (**LFPDPP** is the law's Spanish acronym), came into force in Mexico on 6th July 2010. This law established a general data protection framework, and is the first law of its type at the federal level. It creates a new set of obligations for companies and private entities that collect, process, store or manage personal data, outlining rules, requirements and obligations to ensure proper treatment of personal data. The law applies only to private entities and applies to the processing of personal data by companies and individuals on Mexican territory, regardless of where the data subjects reside. This means that Mexican-based internet companies are obliged to

---

[11] Political Constitution of the United Mexican States, available in English at: http://portal.te.gob.mx/sites/default/files/consultas/2012/04/cpeum_ingl_s_reformas_al_30nov_2012_pdf_69279.pdf

[12] Ibid.

[13] Mexican Penal Code, available in Spanish at: http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf

[14] English translation available at: http://www.cybercrimelaw.net/Mexico.html

[15] Federal Transparency and Access to Public Government Information Law, available in Spanish at: http://www.diputados.gob.mx/LeyesBiblio/ref/lftaipg.htm; see also Introduction To Federal Institute For Access To Information And Data Protection, available at: http://www.privacyconference2011.org/includes/IntroductionIFAIIngles.pdf

[16] Political Constitution of the United Mexican States, available in English at: http://portal.te.gob.mx/sites/default/files/consultas/2012/04/cpeum_ingl_s_reformas_al_30nov_2012_pdf_69279.pdf; see also Introduction To Federal Institute For Access To Information And Data Protection, available at: http://www.privacyconference2011.org/includes/IntroductionIFAIIngles.pdf

comply with the law concerning any personal data they collect on non-Mexican users. The law does not, however, extend to the processing of personal data concerning Mexican residents by companies operating outside Mexican territory. The law provides that companies handling personal data must furnish notice to the affected persons, and individuals have rights of access, correction and objection (on "legitimate grounds") to processing or disclosure. In the event of a security breach that would significantly affect individuals, those persons must be promptly notified.

The LFPDPP incorporates data protection principles from the "International Standards on Data Protection and Privacy", including principles of legitimacy, consent, quality, purpose, proportionality and accountability. In sum, these principles ensure that data will be treated for the purposes intended, with full knowledge of the owners. The legislation also gives additional protections to sensitive personal data. Importantly, the law designates the Federal Institute for Access to Information and Data Protection (IFAI) as the guarantor authority which oversees the regulation, verification and adjudication processes, as well as administration of sanctions and penalties.

International obligations related to privacy

Mexico has signed and ratified the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the American Convention on Human Rights.[17] Mexico has signed the United Nations Guidelines for the Regulation of Computerized Personal Data Files.[18]

Areas of Concern

1. Communications surveillance

Despite Mexico's efforts to strengthen and embed protection of personal data both in its constitutional and legislative framework, there are concerns over certain surveillance practices and laws that have come into force since Mexico's last UPR. These surveillance measures have in most cases been implemented for the purpose of combatting crime, in particular violence and criminal activity arising from Mexico's ongoing fight against drug trafficking.

Between March 2011 and March 2012 the Department of Defence entered into contracts with Security Tracking Devices S.A. De C.V., a surveillance technology company based in Mexico, to buy $350 million worth of surveillance software.[19] This software, which is being used by the Mexican army, can mine text messages from mobile phones, intercept voice calls and emails, log instant messages, and even

---

[17] The Convention is available at: http://www1.umn.edu/humanrts/oasinstr/zoas3con.htm

[18] The Guidelines are available at: http://www.unhcr.org/refworld/pdfid/3ddcafaac.pdf

[19] Ryan Gallagher, Slate, Mexico Turns to Surveillance Technology To Help Fight Drug War, 3rd August 2012, available at: http://www.slate.com/blogs/future_tense/2012/08/03/surveillance_technology_in_mexico_s_drug_war_.html; these secret contracts were published by El Universal newspaper in July 2012, available at: http://www.eluniversal.com.mx/graficos/pdf12/contrato_SDN.pdf

covertly turn on a mobile phone's microphone.[20] The Mexican Department of Defense has confirmed these contracts.[21] However, there is in general a lack of information and transparency surrounding the purchase and use of surveillance software by the Mexican government.

Mexico has had ongoing support from the United States in its war against drug trafficking. According to a report by Aljazeera[22] the US Bureau of International Narcotics and Law Enforcement Affairs said it would contract with the Mexican government to upgrade a surveillance system from 30 to 107 monitoring centres. The system was installed by a New York-based company called Verint in 2006, and can intercept communications from "national telephonic and other communications service providers in Mexico".[23]

The purported objective of these surveillance practices is reportedly to deter drug trafficking, terrorism and other serious crimes, by bolstering Mexico's Public Security Secretariat.[24] However, intrusive and sophisticated surveillance technology of this kind is an incredibly powerful tool in the hands of government and potentially subject to serious abuse. Although judicial approval is required for interception of communications in Mexico, there are concerns that this is being circumvented in the case of surveillance equipment. In addition, given the practice of infiltration of law enforcement agencies by drug cartels,[25] it is feared that this surveillance equipment will be deployed by corrupt authorities to monitor political opponents of anyone deemed a threat to drug cartels' grip on power, and so will be used to commit, rather than combat, crime.

In March 2012 Mexico adopted **surveillance legislation (Ley Geolocalización MX)** that grants the Mexican government/law enforcement authorities the right to collect, without warrant and in real-time, user geographical data from cell phones.[26] There is significant potential for abuse under this law, and the Mexican government is seemingly insensitive to the fact that most mobile phones today transmit continuous and detailed

---

[20] Ryan Gallagher, Slate, Mexico Turns to Surveillance Technology To Help Fight Drug War, 3rd August 2012, available at: http://www.slate.com/blogs/future_tense/2012/08/03/surveillance_technology_in_mexico_s_drug_war_.html; see also Rebecca Fisher, Corporate Watch, Tinker, taylor, cyber spy: On modern surveillance technologies, 2012, available at: http://www.corporatewatch.org.uk/?lid=4440

[21] Ryan Gallagher, Slate, Mexico Turns to Surveillance Technology To Help Fight Drug War, 3rd August 2012, available at: http://www.slate.com/blogs/future_tense/2012/08/03/surveillance_technology_in_mexico_s_drug_war_.html

[22] Katitza Rodriguez and Rebecca Bowe, AlJazeera, How the US fuels Latin America's surveillance technology, 21st May 2012, available at: http://www.aljazeera.com/indepth/opinion/2012/05/201251413563152746 4.html

[23] Ibid.

[24] Ibid.

[25] John Burnett and Marisa Peñalosa, NPR, Mexico's Drug War: A Rigged Fight?, 19th May 2010, available at: http://www.npr.org/templates/story/story.php?storyId=126890838

[26] Lisa Brownlee, National Human Rights Commission – Mexico (CNDH), Re: Mexico law revisions – Warrantless Real-time Cell phone Geolocation Data Surveillance – Parliamentary Gazette Volume X, Number 3455-II, Tuesday, February 21, 2012 (hereinafter "LeyGeolocalización MX"), 24th April 2012, available at: http://static.arstechnica.net/2012/04/24/brownlee.mexico.geoloc.pdf; see also Katitza Rodriguez, Electronic Frontier Foundation, Mexico Adopts Alarming Surveillance Legislation, 2nd March 2012, available at: https://www.eff.org/deeplinks/2012/03/mexico-adopts-surveillance-legislation

data about users' location, meaning that the police will have access to very comprehensive and pervasive data. The legislation is intended to enable the government "to investigate possible crimes more effectively".[27] However, without adequate safeguards, such legislation, which endows government authorities with broad surveillance powers, compromises Mexican citizens' right to privacy, and is in any event an inappropriate and disproportionate response to the intended purpose. The technological reform enabling real-time data location collection can be easily circumvented by cartels and/or organised crime groups infiltrating law enforcement agencies, thus putting Mexican citizens at risk of serious and unchecked violation of their right to privacy.[28] The Mexican Ombudsman has recently filed an unconstitutionality action against the law.[29]

2. Physical Surveillance

In addition to purchasing mobile phone surveillance technology, it has been reported that the Mexican Department of Defense has also purchased **radar scanners**, which enable authorities to see through walls.[30] According to a report, radar scanners have been available to governments for several years, but little is known about how and when they are used.[31] It is reported that some radar scanners are capable of detecting movements through concrete walls from up to 60 feet away.[32]

There are reports that **US Customs and Border Protection drones** are being used in surveillance flights to track drug traffickers on the US-Mexico border.[33] These drones are capable of penetrating deep into Mexican territory and tracking criminals' communications and movements, and are being used to gather information requested by the Mexican government. The drones are equipped with cameras that are capable of identifying very small objects and providing real-time images to ground control operators, and can fly for up to 30 hours without having to refuel, covering up to 40,000

---

[27] Mexico Parliamentary Gazette, year XV, Issue 3455-II, Tuesday, February 21, 2012, available at: http://gaceta.diputados.gob.mx/Gaceta/61/2012/feb/20120221-II.html

[28] Lisa Brownlee, National Human Rights Commission – Mexico (CNDH), Re: Mexico law revisions – Warrantless Real-time Cell phone Geolocation Data
Surveillance – Parliamentary Gazette Volume X, Number 3455-II, Tuesday,
February 21, 2012 (hereinafter "LeyGeolocalización MX"), 24th April 2012, available at: http://static.arstechnica.net/2012/04/24/brownlee.mexico.geoloc.pdf

[29] Mexican National Human Rights Committee, The CNDH Presents an Unconstitutionality Action Concerning Geolocalicion, 13th May 2012, available at: http://www.cndh.org.mx/sites/all/fuentes/documentos/Comunicados/2012/COM_2012_120.pdf

[30] Ryan Gallagher, Slate, Mexico Turns to Surveillance Technology To Help Fight Drug War, 3rd August 2012, available at: http://www.slate.com/blogs/future_tense/2012/08/03/surveillance_technology_in_mexico_s_drug_war_.html

[31] Ibid.

[32] Ibid; see also Emily Finn, MIT News, Seeing Through Walls, 17th October 2011, available at: http://web.mit.edu/newsoffice/2011/ll-seeing-through-walls-1018.html

[33] Ginger Thompson and Mark Mazzetti, The New York Times, US Drones Fight Mexican Drug Trade, 15th March 2011, available at: http://www.nytimes.com/2011/03/16/world/americas/16drug.html?pagewanted=all&_r=0; http://articles.washingtonpost.com/2011-12-21/world/35285176_1_drone-caucus-predator-drone-domestic-drones; Olga Rodriguez, Huffington Post, Mexico: US Drones Allowed Into Its Territory, 16th March 2011, available at: http://www.huffingtonpost.com/2011/03/16/mexico-us-drones-allowed-_n_836649.html

square miles of territory a day. They cannot be easily perceived by Mexicans on the ground.[34] US President Barack Obama and Mexican President Felipe Calderon formally agreed to continue these surveillance flights at a meeting in Washington DC on 3rd March 2011.[35] However, these operations have been kept secret because of legal restrictions in Mexico: the Mexican Constitution prohibits foreign military and law enforcement authorities from operating in Mexico except in extremely limited circumstances. The legality of these drone operations is thus questionable. It is clear that the use of drones poses a serious threat to the privacy rights of Mexican citizens.

Areas of Improvement

The insertion of a paragraph into Article 16 of the Mexican Constitution of 1917, which provides for the protection of personal data and grants citizens the power to oppose disclosure of, and cancel, his/her data is a significant and substantive **additional constitutional protection** of the right to privacy. This protection is enhanced by the addition of clause XXIX-O in Article 73 of the Constitution, which grants the government the power to protect, and regulate the use of, personal data handled by private parties.

The introduction of the **Mexican Federal Law for the Protection of Personal Data in Control of Private Persons**, discussed above, is a significant and comprehensive piece of legislation which enables citizens to enforce their right to protect their personal data. The law reflects the habeas data concept: the individual whom the personal data concerns is designated the "data owner" and is in possession of all relevant legal rights relating to use of that data. The law effectively addresses the various and important factors relating to data protection, including notice, purpose, consent, security, disclosure, access, and accountability. The legislation is in line with the EU Data Protection Directive and the Canadian federal PIPEDA legislation in requiring a lawful basis such as consent or legal obligations for collecting and disclosing personal data.[36] As noted above, the law also incorporates principles from the "International Standards on Data Protection and Privacy", including principles of legitimacy, consent, quality, purpose, proportionality and accountability. Additional protections are given to sensitive personal data, as in the EU Data Protection Directive. Sensitive data is defined as that concerned with the most intimate aspects of a person's life and that which involves a serious risk of discrimination, such as data relating to race or ethnicity, genetics, health, sexual preference, religious or philosophical beliefs, political views, and trade union membership.

---

[34] Ginger Thompson and Mark Mazzetti, The New York Times, US Drones Fight Mexican Drug Trade, 15th March 2011, available at: http://www.nytimes.com/2011/03/16/world/americas/16drug.html?pagewanted=all&_r=0; http://articles.washingtonpost.com/2011-12-21/world/35285176_1_drone-caucus-predator-drone-domestic-drones

[35] Ibid.

[36] W. Scott Blackmer, Information Law Group, Mexico's New Data Protection Law, 28th July 2010, available at: http://www.infolawgroup.com/2010/07/articles/privacy-law/mexicos-new-data-protection-law/

Recommendations

We recommend that the Government of the United Mexican States:

- Ensure that the use of surveillance software is strictly regulated and monitored by the Department of Defense and overseen by judicial and other independent authorities;

- Ensure that appropriate mechanisms and reviews are put in place to guarantee that use of surveillance software is and remains necessary, legitimate and proportionatel

- Demonstrate transparency with respect to the purchase and use of surveillance software by government authorities;

- Repeal the Ley Geolocalizacion MX, or amend it such that government authorities are required to obtain a judicial warrant before being able to access geolocation data;

- Be transparent about the purchase and use of radar scanners by government authorities, including how and under what circumstances they will be used, and what safeguards have been put in place to ensure their proper use;

- Strictly regulate the use of drones, ensure that their deployment is continually overseen and authorised by judicial and other independent authorities, and publicise information concerning their use.