State of Privacy Argentina

1 Argentina
2 Introduction
3 Right to Privacy
4 Communication Surveillance
5 Data Protection
6 Identification Schemes
7 Policies and Sectorial Initiatives

Introduction

Acknowledgement

The State of Privacy in Argentina is the result of an ongoing collaboration by Privacy International and Asociación por los Derechos Civiles (ADC).

Last modified:
Tuesday, March 14, 2017 - 14:20

Right to Privacy

The constitution

While Argentina's constitution does not mention the word ‘privacy,’ it does refer to ‘private actions’ in Section 19, which, according to the Argentine Supreme Court, is the basis of the right to privacy. The section states: "The private actions of men which in no way offend public order or morality, nor injure a third party, are only reserved to God and are exempted from the authority of judges. No inhabitant of the Nation shall be obliged to perform what the law does not demand nor be deprived of what it does not prohibit."

In addition, Section 18 of the Constitution states: "the domicile may not be violated, as well as the written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed."

Regarding data, Section 43 reads: "any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired."

Regional and international conventions

Argentina has ratified a number of international human rights treaties with privacy implications. These include:

- The Universal Declaration of Human Rights;
- The International Covenant on Civil and Political Rights;

- The American Convention on Human Rights; and
- The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families. They all have been accorded the same legal weight as the Argentine constitution (Section 75.22).

Communication Surveillance

Introduction

The total population of Argentina was over 43.6 million in January 2016. 34.8 million Argentines are active Internet users, which corresponds to approximately 80 % of the population. Between January 2015 and January 2016, the number of active Internet users grew 8 %, according to a report by We Are Social. The total number of mobile connections in Argentina is 61.4 million, and 28 million Argentines are active mobile Internet users.

There are 27 million active social media accounts in Argentina, a figure which grew 35 % in the last year. According to a survey gathered by GlobalWebIndex, 37 % of Argentines use WhatsApp, 42 % own a Facebook account, and 20 % own a Google+ account.

Surveillance laws

The relevant statutory provisions governing telecommunications, communications interception and monitoring, data protection and cybercrime are:

- the Civil and Commercial Code, Section 1770;

- the Penal Code, Sections 153, 153 bis, 155, 157, 157 bis, 173.16, 183, 184 and 197 (as amended by Act no. 26.388 or Cybercrime and Violation of Privacy Act);
- the Argentina Digital Act (Act no. 27.078);
- the Intelligence Act (Act no. 25.520), as amended by the Federal Intelligence Agency Act (Act. no. 27.126);
- the Data Protection Act (Act no. 25.326); and
- the Telecommunications Act (Act no. 19.798).

The new law on telecommunications (Argentina Digital Law) does not completely replace the old Telecommunications Act, but instead it establishes in Section 89 that: 'Law 19.798 and its amendments remain in force only with respect to those provisions that do not contradict the provisions of this law.' It is uncertain which provisions remain thus in force.

Surveillance actors

The main laws and decrees setting out the powers and structure of the intelligence and security services are:

- the Creation of the Federal Intelligence Agency (Act No. 27.126);
- the Decree 1311/2015; and
- the Decree 656/2016

Security and law enforcement agencies

The Secretariat of Intelligence was founded in 1946 by General Juan Perón as the Information Coordination Secretariat of State (Secretaría de Coordinación de Informaciones del Estado, CIDE) (National Decree 337/1946). It was a civilian intelligence agency whose

mission was to provide both internal and foreign intelligence. It evolved into a secret police force during Argentina's Military-Civic Dictatorship (1974-1983) and was used by the military junta to track down opponents and spy on 'subversives', including trade union and other left-wing activists.

The Secretariat survived the transition to democracy in 1983. However, following the end of the military dictatorship, the new government was dedicated to clearly redefining the government-military relationship in order to prevent the military from ever again cracking down on political dissidents. This distinction between the two bodies in charge of security – the army and the police – was used as a basis to distinguish between two forms of intelligence.

The 2001 Intelligence Act created the National Intelligence System, which comprised three institutions: the Secretariat of Intelligence, the National Directorate of Military Strategic Intelligence (Dirección Nacional de Inteligencia Estratégica Militar) and the National Directorate of Criminal Intelligence (Dirección Nacional de Inteligencia Criminal). The last two bodies reflect the mentioned distinction between two forms of intelligence. However, the distinction was purely formal and organisational, as the Intelligence Act placed the two directorates under the responsibility of the Secretariat of Intelligence, which was the higher body of the National Intelligence System.

The Intelligence Act was amended in March 2015 by the Federal Intelligence Agency Act. The amendment law created the Federal Intelligence Agency (AFI), which replaced the Secretariat of Intelligence as the highest body of the National Intelligence System. The latter remains essentially the same.

The AFI has two main functions:

1 The production of national intelligence through the

collection, compilation and analysis of information related to the facts, risks and conflicts affecting national defense and internal security. The AFI shall fulfill this function through the bodies that are part of the national intelligence system.

2 The production of criminal intelligence relating to complex crimes relating to terrorism, drug trafficking, arms trafficking, human trafficking, cybercrime, and against economic and financial order, as well as crimes against public authorities and the constitutional order. The AFI shall fulfill this function through its own means for collecting and gathering information.

The AFI is led by a Director General with the rank of Minister, appointed by the President of Argentina with the approval of the Senate. The Deputy Director, with the rank of State Secretary, is appointed in the same way.

The National Directorate of Criminal Intelligence is placed under the Ministry of Security and is limited to criminal intelligence (Section 9). Following the division among police forces, the directorate is composed of the Intelligence Federal Police, the Intelligence National Gendarmerie, the Intelligence Naval Prefecture and the Intelligence Provincial Police Forces. The head of the Directorate is appointed by the Minister of Interior.

The National Directorate of Military Strategic Intelligence is placed under the responsibility of the Ministry of Defense and is strictly restricted to foreign counterintelligence. Following military divisions, the directorate is composed of the Intelligence Chief of Staff, the Intelligence Army, the Intelligence Navy and the Intelligence Air Force. The head of the Directorate is appointed by the Minister of Defense.

The Argentine President sets the strategic guidelines and

objectives of national intelligence.

Before the institutional change, Eduardo Estevez had remarked that while each body of the National Intelligence System had clearly described responsibilities, in reality the scheme made the most important agency – the Secretariat of Intelligence – the only body that was truly expected to be held accountable. As the AFI has only recently started to function, it is still not clear whether the responsibilities of each of the institutions of the National Intelligence System will continue to be blurred.

Finally, the Intelligence Act provides that the National Intelligence System bodies must not:

- Perform repressive activities, fulfill police functions or conduct criminal investigations unless so required by justice with respect to a judicial proceeding or when so authorised by law.
- Obtain information, produce intelligence or store data on individuals because of their race, religion, private actions, and political ideology, or due to their membership in partisan, social, union, community, co-operative, assistance, cultural or labor organisations, or because of legal activities performed within any field.
- Exert influence over the institutional, political, military, police, social and economic situation of the country, its foreign policies, or over public opinion, individuals, media, or any kind of association.

All the activities of the intelligence agencies must also respect the Data Protection Law.

Budget

The Executive Power is expected to include in the yearly budget a line on 'Intelligence' under the topic 'Defense and

Security Services'. This budget contained no detail nor did it mention how much was allocated to each body within the National Intelligence System, which led to a discretionary use of the budget and corruption within the intelligence services. Thus, Young holds in Código Stiuso that:

"[The Secretariat of Intelligence] ... does not account for its fund expense. On what is the intelligence budget spent? Nobody knows, except from a few people inside *La Casa*. In 2003 ... the budget of the Secretariat of Intelligence was 238 million pesos. More than 650 thousand pesos per day. But… the accounts cannot explain those amounts. The SI spent 79 million annually in wages, an average of 2,530 pesos a month per employee. That information could not be adulterated: funds that flowed in wages could not be modified, because salaries were mostly paid officially. About the remaining 159 million, however, there was no information. That amount was destined to electricity, gas for cars, phones… the overall functioning of La Casa. But 159 million were many millions. There were too many [for those expenses]. The only form of accountability for those funds … was a modest list consisting on a single sheet of paper that was sent to the National Congress. A list with objectives that were too ambiguous…: [it was stated] that [the budget] was invested in wiretapping, in investigations linked to smuggling and drug trafficking, in the maintenance of secret bases and cars, and in daily expenses. Approximate sums, without any detail, impossible to control, certainly false."

Consequently, the Federal Intelligence Agency Act passed in March 2015 added the following provision to the Intelligence Act: 'The items on the budget determined by the Executive Branch for the agencies of the National Intelligence System … shall be public ... Only the funds necessary for intelligence whose publicity could affect its normal functioning may be kept confidential. Such funds shall be subject to the controls of this law. The National Intelligence System bodies shall ensure transparency in the management of confidential

funds. To this end, they shall establish appropriate [accountability procedures], provided [the procedures] do not affect the safety of the intelligence activities and of those who take part in them' (Section 38 bis).

A joint committee formed by members of the Senate and the Chamber of Deputies is in charge of the control and oversight of the budget and expenditures.

Each directorate has to inform their respective ministry of their required budget and is responsible for spending it.

In May 2016, the Decree 656/16, issued by the Executive, abrogated annexes II to VII of the National Intelligence Doctrine (Decree 1311/15), effectively eliminating the personnel regime, the organic and functional structure, and the budget administration scheme for AFI established by the Intelligence Doctrine, returning to the so called "discipline of secrecy" already established in Decree 950/2002; and with the elimination of the budget administration scheme, removing the distinction between public and reserve funds, all of AFI's budget becomes secret.

Interception of communications

The creation of the AFI was accompanied by the separation of the interception capabilities from this intelligence body into a new entity, the Department for Interception and Captation of Communications (Departamento de Interceptación y Captación de las Comunicaciones, DICOM) under the orbit of the Public Ministry, as the only state entity allowed to conduct the communication interceptions authorized by the competent judicial authority. By December 2015, the Executive issued Decree 256/15, establishing the transfer of DICOM to the orbit of the Supreme Court, and in 15 February 2016 the Supreme Court created the Directorate of Monitoring of Communications (Dirección de Captación de Comunicaciones, DCC) replacing DICOM.

In September, the Supreme Court passed Acordada 30/2016, creating the Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado del Poder Judicial de la Nación, which will be in charge of the DCC.

Surveillance capabilities

Several reports emerged over the past few years documenting a system that differed substantially from what was indicated in the law. According to Gerardo Young in his book *La Argentina Secreta*, phone providers were paid millions of US dollars each year to set up interception systems. Nokia Siemens Network also reportedly was providing a Data Voice Call Recording and Acquisition Unit to Argentine phone providers and that the intelligence services had offices within the headquarters of phone providers to conduct interceptions. Jaime Stiuso, an intelligence agent attached to the Argentine intelligence services, was exposed as the most powerful spy in Argentina for years, having managed the former Secretariat of Intelligence mostly outside of what was prescribed by law.

Further scandal erupted in 2015 when Alberto Nisman, a prosecutor that had been carrying out the judicial investigation of Iran's involvement in the attack against the Argentine Israelite Mutual Association of Buenos Aires in 1994, was found dead in his apartment on 18 January. It is alleged that during a 10-year investigation, Nisman had gathered phone recordings that revealed an impunity deal between the Iranian and Argentinian governments in exchange for economic benefits. Nisman worked closely with Jaime Stiuso during his investigations, and it is alleged that the intelligence services were involved in his death.

Technologies

In March 2014, a security and surveillance technology conference called Segurinfo was held in Buenos Aires, and in September 2015 Buenos Aires held another conference called Seguriexpo. Among the government members who attended Segurinfo was Sergio Blanco head of the Secretary for Management Technology. Among the companies present at Segurinfo were Dreamlabs, Widefence (a Blue Coat reseller), Blue Coat, Cisco, Alcatel-Lucent and 3M. Furthermore, Utimaco and Blue Coat are companies with offices in Argentina.

A parliamentary inquiry in Germany had revealed that over the past decade the German government had sold surveillance technologies to Argentina.

In July 2015, after the leak of internal information from the Italian spyware vendor Hacking Team, it was established that the company negotiated with several intermediaries in Argentina that said to have ties to Law Enforcement Agencies and State intelligence bodies, but it is not clear from the leaked emails that a commercial transaction actually took place.

Surveillance oversight, checks and balances

The Ministry of the Interior and Transport and the Ministry of Security largely oversee national security issues. There is also Congress' Bicameral Commission 'Commissión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia del Honorable Congreso de la Nación'.

Surveillance case law

The Argentine Supreme Court has held that the right

to privacy and intimacy has its constitutional basis in Section 19 of the Constitution and that the right protects a wider sphere beyond domestic and family life. It has further stated that no one can interfere in the private life of a person or in areas of his or her activity that are not intended to be made public without his or her consent. Only by statute can such interference be justified, provided that there is an overriding interest in safeguarding the freedom of others, the defense of society, morals or prosecution of crime.

Recent cases involving Google and other search engines have ruled on the constitutional right to privacy. On 27 October 2014, the Supreme Court declared that in most cases search engines are not liable for linking to content that could violate the constitutional right to privacy. The Court held that to establish the liability of search engines it must be shown that the wrong was committed with intention or negligence, and added that "search engines have no general obligation to monitor ... the contents that are uploaded to the Internet ... the engines are, in principle, not liable for content they did not create." However, "there are cases in which the search engine can become liable for content that [it did not create]: this will happen when it has actual knowledge of the unlawfulness of certain content, if such knowledge is not followed by a diligent act."

In Argentina, metadata is protected to the same degree and using the same legal basis as content. In 2009, the Inter-American Court of Human Rights held in its judgment on the 'Escher v. Brazil' case that:

"[The right to privacy] applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by taping it and listening to it, or 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."

In 2009, the Argentine Supreme Court also asserted in the case 'Ernesto Halabi v. PEN' that the collection of metadata must comply with the rules regarding the interception of content. Citing the former Telecommunications Act, which contained a similar general principle to the Argentina Digital Act, and Section 236 of the Penal Procedural Code, which sets out the same procedure for the request of communications interception and of metadata, the Court held that 'telephone communication registers for the purpose of criminal investigation ... are subjected to restrictions in this area similar to those that exist regarding the interception of the content of written or telephone communications.'

While the law does not require telecommunication companies to collect and store metadata, they are allowed to do it and may have been doing so in the past.

Examples of surveillance

In November 2011, Argentine newspaper Página 12 revealed the existence of a database called Proyecto X (Project X), originally created to gather data on drug dealers and address complex crimes in 2002 and updated in 2006. However, Proyecto X was revealed to have been used to target left-wing activists and trade

unionists. The project gathers as many personal details as possible on individuals. This includes general information such as addresses, bank details, properties, political affiliations and also private information such as sexual preferences, and whether the person smokes or not. Reports have also revealed that policemen infiltrated protests and political meetings to gather that information. In February 2012, the government replied to pressing questions on the matter by claiming that Proyecto X was 'almost obsolete.'

Left wing activists, however, still feel targeted by the government. Speaking to Privacy International, human rights lawyer Nicolas Tauber says he has encountered several cases of people who had received voicemail messages containing tapped phone conversations they had had in the past. He also said that there has been multiple instances of human rights lawyers who had been victims of burglary and only the electronic devices had been taken. He said his own office had been targeted and while the other lawyers, who do not work on human rights issues, had not had anything stolen, his own USB sticks had disappeared.

Data Protection

Data protection laws

The Data Protection Act seeks to establish 'the comprehensive protection of personal data in files, registers, data banks or other technical means for data processing, whether public or private …, to ensure the right to … privacy of individuals, as well as the access to the information that is held about them,

in accordance with the provisions of Section 43 … of the Constitution' (Section 1).

The Act also states that 'the processing of personal data is unlawful when the data subject has not given his or her express consent, which must be done in writing, or through any other similar means' (Section 5.1).

Section 11.3 diminishes the requirement for consent when data is procesed by agencies of state bodies in compliance with their respective powers.

Section 23 of the Act sets out the treatment of personal data when it is stored for law enforcement and intelligence purposes, as stated in the previous section.

Access to stored data

According to the Intelligence Act, judicial authorization to intercept communications shall be granted for a period that must not exceed sixty days. When it is necessary to complete the investigation, the period can be extended by the judge for a maximum of another sixty days. Once these time limits have passed, the judge shall order the initiation of a judicial case or otherwise order the destruction or deletion of the information and recordings obtained through the interception.

Section 23 of the Data Protection Act sets out the treatment of personal data when it is stored for law enforcement and intelligence purposes:

"1. [The Data Protection Act shall be applied to] personal data which on account of their storage for administrative purposes must be subjected to permanent registration in the data banks of the armed forces, security forces, police or intelligence agencies; [the same principle applying to] data on personal background provided by the said banks to the administrative or judicial authorities that may require them by virtue of legal provisions.

2. The treatment of personal data with national defense or public security purposes by the armed forces, security forces, police or intelligence agencies, without the consent of the parties concerned, is limited to those cases and categories of data as are necessary for the strict compliance with the duties legally assigned to such bodies for national defense, public security or the punishment of crimes. In those cases, files must be specific and formed for the said purpose, and they shall be classified by categories, depending on their degree of reliability.

3. Personal data registered with police purposes shall be erased when deemed unnecessary for the inquiries which gave rise to their storage."

Accountability mechanisms

The regulatory body overseeing data protection in Argentina is the Argentine Personal Data Protection Agency (Dirección Nacional de Protección de los Datos Personales, DNPDP). The DNPDP's functions are extremely broad and it was designed to be an independent agency with financial self-sufficiency and with a structure necessary in order to perform such functions properly. A partial list of its functions includes providing advice for citizens, regulating powers, controlling and registerin public and private databases and applying sanctions upon default, with a broad jurisdiction throughout the country. However, the agency operates with a relatively low budget and a limited number of staff. As a result of these constraints, the DNPDP has not been able to fully perform its functions and in particular has exercised limited control over the treatment and use of

personal data by the state authorities.

Data breaches: case law

Our research has not yet shown any case law related to data breaches in Argentina. Please send any tips or information to: research@privacyinternational.org

Examples of data breaches

In late 2014, following the October elections, a blogger identified a code that was then used by a programmer to set up a site that enabled images to be retrieved from the the electoral registry. After this reached public attention through media reporting, the photographs were taken down.

In July 2016, the Chief of Minister Cabinet issued the Resolution 166/2016 whereby the National Administration for Social Security (ANSES) would share its database (containing data such as name, identity card number, home address, phone number, email address, date of birth, and marital status) with the Secretariat of Public Communication, which is functionally reliant on the Chief of Minister Cabinet, in order to improve the government's communication strategy. The decision was contested by experts on data protection law and members of opposition parties, who alleged that the data transfer does not align with the finality principle, because the data were collected for an efficient operation of the social security system, not for communication or public relations activities.

A lawsuit was filed by an Argentine citizen, who argues that the Resolution is contrary to the Constitution, because it affects her right to privacy. The case is still pending.

Identification Schemes

ID cards and databases

Since 1968, Argentine citizens are obliged to acquire a National ID card (DNI, Documento Nacional de Identidad) from the National Citizen's Registry (RENAPER, Registro Nacional de las Personas), an agency under the Ministry of Interior. In 2014, RENAPER issued Resolution 3020/14 in which it established that the only valid identification document is the new digital ID card, and that the citizen's biometric data will be digitised and collected into a unified database. Since November 2009, RENAPER has issued more than 41 million new ID cards. The database in question is the Federal Biometric Identification System for Security or SIBIOS (Sistema Federal de Identificación Biométrica para la Seguridad), created in 2011 by Executive Order 1766/11 under the Ministry of Security. The biometric data collected by SIBIOS consists mainly of fingerprints and facial patterns. The main users of SIBIOS are the Federal Police, the National Gendarmerie, the National Coastguard, the Airport Security Police, RENAPER and the National Immigration Directorate.

Voter registration

Our research has not yet shown any privacy issues related to voter registration in Argentina. Please send any tips or information to:

research@privacyinternational.org

SIM card registration

Law 25/891 from 2004 on Mobile Communications Services mandates the registration of all mobile phone users.

In April 2016, the Minister of Security announced that the Ministry would start a joint work with the Ministry of Communications to create a national registry of SIM cards in order to remove stolen phones from the market as well as to render them useless with the help of telephone companies.

Policies and Sectorial Initiatives

Cybersecurity policy

In 2011, by Resolution 580/11, the Critical Infrastructure of Information and Cybersecurity Program (Programa de Infraestructuras Críticas de Información y Ciberseguridad, ICIC) was created under the Chief of Staff's office. The Program is responsible for the development of a specific regulatory framework conducive to the identification and protection of critical infrastructure and critical entities and jurisdictions throughout the national public sector, interjurisdictional agencies and the civil and private sector organizations.

In June 2015, by the Decree 1067/15, the Executive establishe an Undersecretary position for the Protection of Critical Infrastructure of Information and Cybersecurity, under the Cabinet Secretariat in the orbit of the Chief of Staff's office. The Undersecretaru os ssigned with similar

tasks and objectives as the ICIC Program; according to the Decree, the Program was transferred to the National Directorate of Critical Infrastructure of Information and Cybersecurity within the Undersecretary.

By the beginning of 2016, the Executive branch issued Decree 13/16 creating the new Ministry of Modernization, and within it the Undersecretary of Technology and Cybersecurity, which encompasses the various State bodies mentioned above and puts it in charge of the National Office of Information Technology (Oficina Nacional de Tecnologías de Información, ONTI), the National Directorate of Infrastructure and Operations (Dirección Nacional de Infraestructura Tecnológica y Operaciones), and the National Directorate of Critical Infrastructure of Information and Cybersecurity (Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad).

The new Undersecretary of Technology and Cybersecurity is in charge of, among other things, developing a national strategy for technological infrastructure and the protection of critical information infrastructure and cybersecurity at the national level; understanding and dictating policies, standards and procedures of technology and information security; as well as understanding processes related to the actions of the national computer security incident response team.

As of August 2016, Argentina does not have a national cybersecurity strategy.

Cybercrime

In June 2008, the Cybercrime and Violation of Privacy Act was adopted. It introduced several reforms to the Penal Code.

Currently, cybercrime and crimes regarding unlawful

surveillance of communications are provided for in the Penal Code, which applies at a national level. Among others, the following conduct constitutes a crime:

- Unlawfully accessing a telephone or electronic communication or a letter (Section 153);
- Accessing by any means a computer system or computer data which is subject to restricted access, without authorization or exceeding the conferred authorization (Section 153 bis); and
- Accessing, whether unlawfully or by breaching a system of confidentiality and security of data, a personal data bank (Section 157 bis).
- Sexual grooming of an underage person through electronic communications, telecommunications or other data transmission technology (Section 131).

Penalties for unlawfully accessing data or communications are more severe when the offender is a public official or employee abusing his or her authority.

Encryption

Our research has not yet shown any privacy issues related to encryption in Argentina. Please send any tips or information to: research@privacyinternational.org

Licensing of industry

Until recently, the telecommunications industry in Argentina was regulated by Secretariat of Communications (Secratarí a de Comunicaciones, SECOM) and the National Communications

Commission (Comisión Nacional de Comunicaciones, CNC).

The Argentina Digital Act, passed on 16 December 2014, established that the Federal Authority for Information Technology and Communications (Autoridad Federal de Tecnologías de la Información y las Comunicaciones, FAITC) would continue with the tasks formerly carried out by SECOM and CNC (conf. Section 79).

FAITC is in charge of:

- Regulating, controlling and monitoring ICT in general (including postal service);
- Promoting and regulating access to ICT and telecommunications services, including broadband and Internet;
- Granting and declaring the expiration of the licenses and permits for telecommunication providers; and
- Ensuring that companies meet the expected quality standards.

As regards communications surveillance, the Argentina Digital Act requires licensees of ICT services to guarantee the confidentiality of users' transmitted messages and the secrecy of communications, as well as to meet the requirements on national defense and public safety made by the competent authorities. The FAITIC can impose sanctions on licensees who fail to meet these obligations.

On 30 December 2015, the government unified the Autoridad Federal de Servicios de Comunicación Audiovisual – the agency in charge of regulating television and radio services – and FAITIC to create the ENACOM (Ente Nacional de Comunicaciones or National Communications Entity).

Communications Service Providers

In 1990, the Argentine government privatised the state-owned telephone company, Entel. Currently, the top four mobile network operators are Claro (owned by América Móvil), Movistar (owned by Telefónica), Personal (owned by Telecom Argentina) and NEXTEL (owned by NII Holdings).

The main Internet providers are: Fibertel (owned by Grupo Clarin), Arnet (owned by Telecom Argentina) and Speedy (Telefónica).

All companies are privately owned and mostly by foreign companies. Telefónica is Spanish, América Móvil is Mexican, NII Holdings is American and Telecom Argentina is half owned by Telecom Italia (the other half belongs to an Argentine family).

According to the Argentine journalist Gerardo Young's book *Código Stiuso*, phone providers were paid millions of US dollars each year to set up interception systems and to facilitate wiretapping [p.175].

E-governance/digital agenda

On 24 April 2014, SECOM created the Argentine Internet Policy Committee (Comisión Argentina de Políticas de Internet). The committee aims to address issues of internet governance and develop a national strategy regarding the internet.

On 10 December 2015, under Decree 13/2016 President Mauricio Macri created the Ministry of Modernisation. The Ministry is to participate in defining the strategies and standards on information technology, communications and other associated electronic procressing of information from the National Administration. Technology and e-governance are at the core of the Ministry of Modernisation.

The ministry deals with the implementation of new

technologies for the civil service, transparency of process management and training of public employees.

At the moment it is unclear the changes that have taken place as a result of the Ministry of Modernisation's creation that affect the right to privacy but it looks set to play an important role in the future.

Health sector and e-health

Article 13 of Law 26529 regulates the requirements for digital medical records. The law establishes the requirements to preserve the integrity, authenticity, durability and recoverability of health information. Those are, as principles, good for guiding the work but structural issues still exist for the Law to be fully adopted.

Smart policing

Privacy International is not aware of any smart policing issues in Argentina. Please send any tips or information to: research@privacyinternational.org

Transport

On 4 February 2009, by Decree 84/09, the Executive launched a new travel card, the SUBE card (Sistema Único de Boleto Electrónico), under the oversight of the Secretariat of Transportation within the Ministry of Planning.

Although one can buy the SUBE card without an ID card at kiosks throughout the various cities where the system is implemented, a user must register the card and link it to

their personal data, such as name and surname, national ID card, gender, date of birth, email and phone number in order to consult the remaining balance of the card or the journeys made online, or to access the social tariffs available to specific groups like pensioners.

Smart cities

The Ministry of Modernization has Smart Cities as part of its development agenda. It takes into account six dimensions: competitiveness governance the environment human development urban planning Of these, governance which is the area that has the most association with privacy out of the six, is defined as meeting the needs and demands of the population. It is unclear whether the Ministry includes privacy concerns within any of those six dimensions.

Migration

On 13 June 2012, the RENAPER (Registro Nacional de las Personas) issued Resolution 1474/12 establishing a new electronic passport with biometric capabilities. RENAPER's biometric database is part of SIBIOS.

Emergency response

Privacy International is not aware of any privacy issues related to emergency response in Argentina. Please send any tips or information to: research@privacyinternational.org

Humanitarian and development programmes

Privacy International is not aware of any privacy issues related to humanitarian and development programmes in Argentina. Please send any tips or information to: research@privacyinternational.org

Social media

Privacy International is not aware of any privacy issues related to social media in Argentina. Please send any tips or information to: research@privacyinternational.org