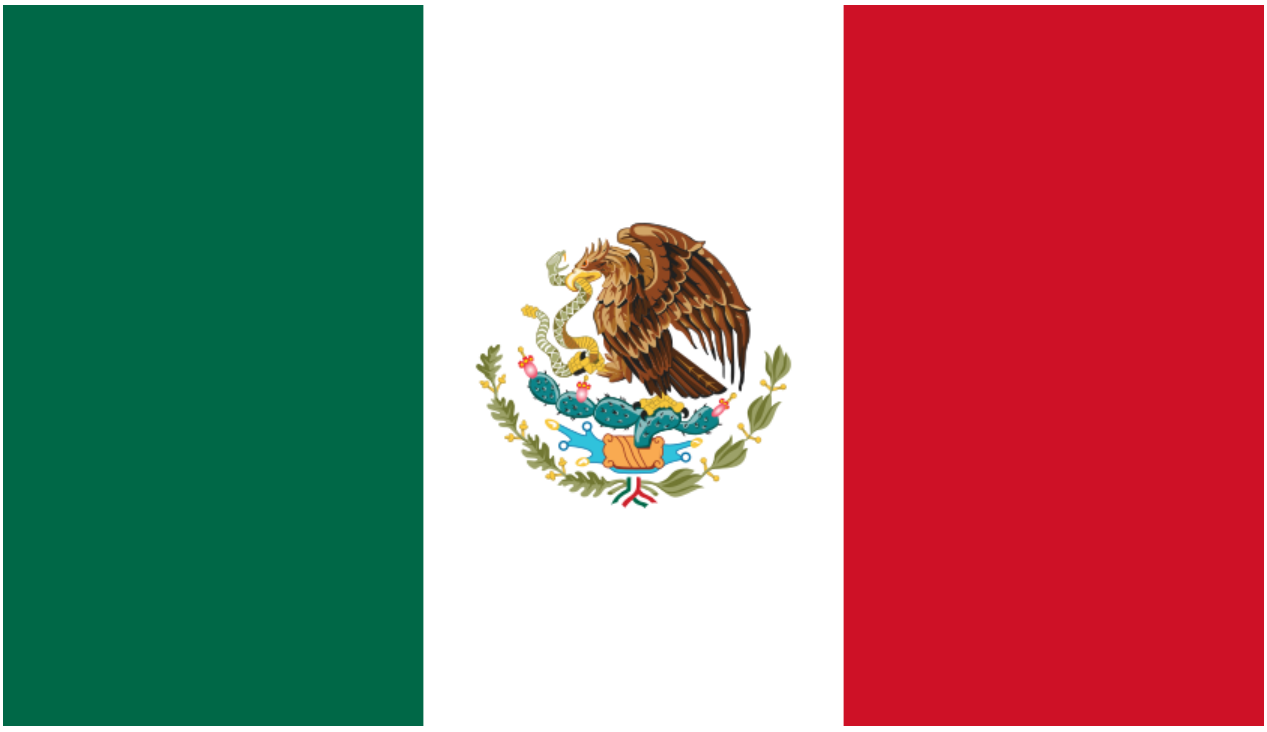
State of Privacy Mexico



January 2018

Table of contents

- **Communication Surveillance**
- **Data Protection**
- **Identification Schemes**
- **Policies and Sectoral Initiatives**

Introduction

Acknowledgement

*The State of Privacy in Mexico is the result of an ongoing collaboration by Privacy International and **Red in Defensa de los Derechos Digitales** (R3D) in Mexico.*

Key Privacy Facts

1. Constitutional privacy protections: The right to privacy is enshrined in article 6 of the Mexican constitution.

2. Data protection law: A number of pieces of legislation regulate data protection in Mexico, primarily the 2010 Federal Law on the Protection of Personal Data held by Private Parties.

3. Data protection agency: The primary data protection agency is the National Institute for Transparency, Access to Information and Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 'INAI').

4. Recent scandals: The Mexican security services have purchased advanced surveillance tools which have been deployed domestically. In 2017, government-exclusive spyware from Israeli firm NSO group was used in an espionage operation targeting Mexican government officials, researchers and public health advocates.

5. ID regime: Mexico's national ID card scheme is called the Unique Population Registry Code (Clave Única de Registro de Población, 'CURP'). It is used for paying taxes, accessing education and military service, among other purposes.

Right to Privacy

The constitution

The right to privacy is enshrined in article 6 of the **Political Constitution of the United Mexican States**, which stipulates that:

"A. In order to exercise the right to information, the Federation, the States and the Federal District, in the sphere of their own cognizance, shall be ruled by the following principles: (...)

II. Information regarding private life and personal data shall be protected according to law and with the exceptions established therein:

Article 16. No person shall be disturbed in his private affairs, his/her family, papers, properties or be invaded at home without a written order from a competent authority, duly explaining the legal cause of the proceeding.

All people have the right to enjoy protection on his personal data, and to access, correct and cancel such data. All people have the right to oppose the 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.(...)"

Regional and international conventions

Mexico has ratified several international instruments relevant to the right to privacy, including:

- **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**.

Communication Surveillance

Introduction

Mexico had a total population of **around 127 million** in 2016. The country had a national internet penetration figure of **around 59.54 % in 2016**. That year, the mobile phone subscription rate was around **88.2 persons per 100**.

According to **a 2015 study by PricewaterhouseCoopers**, Mexicans spend an average of just under four hours per day on social media, and the most popular social media platforms include Facebook, Twitter, Youtube, Google+ and Linkedin.

Surveillance laws

In Mexico, the following laws regulate communication surveillance:

- **National Code for Criminal Procedure** (Código Nacional de Procedimientos Penales)
    - Article 291: Private communications surveillance. This article authorizes the Mexican Attorney General, or the public servants to whom he delegates this faculty, and

his counterparts within each federal entity, to request authorization from the competent judicial authority to intercept communications when the Public Prosecutor deems it necessary, stating the object and necessity of such measure.

- Article 303: Geographic location in real-time and request for disclosure of stored data. This article authorizes the Mexican Attorney General, or the public servants to whom he delegates this faculty, to request the competent judicial authority to require from the telecommunication services providers and/or licensees the disclosure of this type of information, in a timely and sufficient way. This article also establishes that the information should be destroyed in case it does not serve as appropriate or relevant means of proof.

- **Federal Police Law** (Ley de la Policía Federal)

    - Article 8: Among the powers and obligations of the Federal Police, it establishes the requirement "[t]o request, in writing, the judicial authority to authorize private communication surveillance for the investigation of crimes."
    - Article 51: Establishes that preventive communication surveillance shall be authorized only in relation to the commission of the following crimes (from the National Criminal Code):

        - a) Escape of convicts;
        - b) Crimes against health, with some exceptions;
        - c) Corruption of minors or incompetent persons;

- d) Pornography of underage or incompetent persons;
- e) Sexual tourism against underage or incompetent persons;
- f) Sexual trafficking of underage or incompetent persons;
- g) Exploitation of the body of underage or incompetent persons;
- h) Assault committed in highways or roads;
- i) Homicide related to organized crime;
- j) Human trafficking of underage or incompetent persons;
- k) Car theft;
- l) Extorsion;
- m) Money laundering;
- (From the Federal Law for Firearms and Explosives): clandestine insertion of firearms, in terms of the Federal Law Against Organized Crime;
- (From the the General Migration Law): human trafficking of persons without papers, and persons mentioned by the General Law to Prevent and Punish Kidnapping Crimes.

- **National Security Law** (Ley de Seguridad Nacional):
    - Article 34: Authorizes the CISEN to request the judicial authority, in the terms regulated by the Mexican Constitution and this law, to authorise the surveillance

of private communications for those cases which imply threats against National Security. It also defines communication surveillance as the capturing, tapping, monitoring, recording or registering, performed by an authorized entity, of private communications of any kind and by any means, device or technology.

- Article 39: Establishes that surveillance can be applied to private communications or broadcasts, carried out by any means of transmission, whether already known or to be known, or in person, including the recording of private images.

- **Federal Telecommunications and Broadcasting Law** (Ley Federal de Telecomunicaciones y Radiodifusión):

    - Article 189: Establishes that telecommunication licensees and, where applicable, the service providers of apps and content and authorized entities, are obliged to respond to any written request, duly justified by reasons of fact and law, from a competent authority.
    - Article 190: Establishes that telecommunication licensees and, where applicable, the authorized entities, are obliged to (amongst others): (...) II. Maintain a registry and control of communications made through any line, under any method, which allows the identification of listed data. (...) IV. Have a dedicated division, available 24/7, to handle requests for information, geographic localization and private communication surveillance as mentioned above.

- **Federal Law Against Organized Crime** (Ley Federal Contra la Delincuencia Organizada):

- Article 16 (...) Establishes that private communication surveillance covers a whole system of communications, or applications that result from technological evolution, that allow the exchange of data, information, audio, video and messages, as well as electronic archives that record and/or preserve the content of the communications or register data that identifies the communications, which may be presented in real-time or after the communication process has been carried out.
- Article 17: Establishes that the requests for communication surveillance must: be duly justified by reasons of fact and law; state the individual or individuals subject to the measure; identify the place or places where it will be carried out, if possible; identify the type of communication, its duration and the process to be implemented and the lines; identify the numbers or devices that will be tapped and, where applicable, the denomination of the telecommunication service licensee by whom the communication surveillance will be implemented. This article also determines that the time limit of the surveillance, including its extensions, shall not exceed six months. After this period, new communication surveillance shall be authorized only when the Public Prosecutor demonstrates there is new evidence that justifies it.
- Article 24: Establishes that the jurisdictional authority must order the destruction of those registries of communication surveillance that are not related to the crimes investigated or to other crimes that require the opening of a different investigation, unless the defense requests that such information be preserved because it

considers it useful for its work. Also, that the authority should order the destruction of the registries from unauthorized communication surveillance or when these exceed the time limit of the corresponding judicial authorization.

- Article 28: Establishes that any public servant involved in private communication surveillance should maintain discretion about their content of those communications.

- **General Law to Prevent and Punish Crimes of Kidnapping** (Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro):

    - Article 24. Establishes that the Mexican Attorney General, or the public servants to whom he delegates this faculty, his counterparts within each federal entity and the authorities so empowered by law, may request from the federal judicial authority approval to surveil private communications. The request for authorization shall include its legal basis, the reasoning behind its applicability, the type of communications to be tapped, and where applicable, the subjects or the lines, devices, numbers and places that will be surveilled, as well as the time of surveillance, which cannot exceed six months. The investigative authority may use all the technological means it deems necessary to carry out the surveillance. In any case, it is the obligation of the telecommunication services licensees involved to assist in this.

    - This article also states that the disclosure of private communications in application of this law constitutes

an exception to the duty of confidentiality established by other laws.

- The Public Prosecutor may offer to the corresponding judge, as means of proof, the findings revealed by the surveillance. If not admitted, they must be destroyed.
- Finally, the article mentions that any procedure developed in terms of this law, carried out by means of illegal or unauthorized conduct, must be nullified by the respective judge. Article 50 Ter. establishes that authorization for surveillance of private communications, in application of this law, shall be granted only in cases of homicide, assault in highways or roads, car theft, kidnap or illegal detention, the crimes previously mentioned from the Federal Criminal Code as well as from the Law to Prevent and Punish Crimes of Kidnapping and their equivalent crimes regulated by local laws from the federal entities.

- **Guidelines for Collaboration on Security and Justice Matters** (Lineamientos de Colaboración en materia de Seguridad y Justicia). The seventh guideline establishes that the Licensees and Authorized Entities are obliged to designate a division responsible for handling te requests for geographic localization, in real-time, of mobile devices and equipment, and disclosure of stored data and private communication surveillance. This division shall be available 24/7 to attend such requests.
- Proposed **Internal Security Law** (Ley de Seguridad Interior). This proposed law would expand the communications surveillance powers of CISEN, the Center for Research and National Security, an intelligence agency under the Ministry of the Interior. It was approved by the Chamber of Deputies in late November 2017

and has been referred for debate and adoption in the Senate. A wide range of international actors **including the UN Special Rapporteur on Human Rights** has expressed concerns over the draft law.

Surveillance actors

According to the **National Code of Criminal Procedure** (Código Federal de Procedimientos Penales) and applicable legislation, the only authorities empowered to conduct communication surveillance are:

- **The Federal Police**;
- **Center for Research and National Security** (Centro de Investigación y Seguridad Nacional, CISEN); and
- the **Public Prosecutor** agencies.

Surveillance capabilities

Law enforcement access to communications data

The Mexican government appears to have a significant appetite for communications surveillance. Mexican mobile operators fielded **more than 55,000 requests** from authorities for information on citizens' calls, messages, and location data, according to figures obtained by Reuters in 2015. This was nearly 25 percent higher than in 2013.

A report publised by R3D in November 2016 revealed a marked increase in the number of requests by Mexican authorities for access to communications data. The report called surveillance "out of control".

Intrusion malware

ln 2015, files from Italian surveillance technology company **Hacking Team were hacked and released to the public**. Information in the leak

revealed that the following Mexican government agencies purchased technology to intercept private communications:

- The governments of Durango, Querétaro, Estate of Mexico, Puebla, Campeche, Baja California, Tamaulipas, Nayarit, Sonora and Yucatán;
- the Marine Ministry (Secretaría de Marina);
- the Army;
- the Federal Police;
- the Prosecutor's Office of the State of Mexico;
- CISEN; and
- PEMEX (the Mexican oil institution).

The media disclosed that the Mexican government was the number one client of the Italian firm and that among the technologies purchased was Hacking Team's Remote Control System "Da Vinci" product and other malware used to spy social networks and mail services including Facebook, Twitter and Gmail. Also, in 2014, it became public knowledge that the Mexican government acquired technology to bug mobile phones **from the Finnish company NetHawk**. To date, the government has failed to inform the public under which conditions this technology would be used, for what purposes, by which entity and the legal basis of its deployment.

In February 2017, an **investigation by the Citizen Lab** revealed that government-exclusive spyware from Israeli firm NSO group was used in an espionage operation targeting Mexican government food scientists and two public health advocates working to combat obesity. A journalist investigating official corruption, Rafael Cabrera, had also been **targetted with the spyware**. Further details about targets were revealed by **the Citizen Lab** and **R3D** in mid-2017. These **included**

lawyers investigating the mass disappearance of students, an **anti-corruption campaigner**, influential journalists and an American representing victims of sexual abuse by the police, **according to the New York Times**. In December, the UN and IACHR Special Rapporteurs on Freedom of Expression jointly **called on the Mexican government** to establish an independent investigation into the use of the spyware, and to establish a legal framework to protect individuals from arbitrary and clandestine interference in their privacy.

Surveillance oversight, checks and balances

Article 69 of the **General Law for Transparency and Access to Public Information** imposes the duty to those authorities allowed to carry out communication surveillance to publish periodic statistical reports on the purpose, temporal scope and legal basis of:

- The number of surveillance communication requests;
- Access to the communications registry; and
- Access to data regarding the geographic localization of mobile communication devices in real time.

Also, they must include a reference that the corresponding judicial authorization was granted. Moreover, the **Federal Telecommunications Institute** (Instituto Federal de Telecomunicaciones) is in charge of verifying that the telecommunication service providers effectively comply, without undue delay, with their transparency obligations, in accordance to the **Guidelines for Collaboration on Security and Justice Matters** (Lineamientos de Colaboración en materia de Seguridad y Justicia).

Surveillance case law

In April 2016, the Second Chamber of the Supreme Court of Mexico

rejected a legal challenge to the data retention provisions of the Federal Telecommunications Act (also known as the 'Ley Telecom') requiring all telephone companies and internet service providers to retain users' communications data for 24 months. The **challenge had been filed** by the **Red en Defensa de los Derechos Digitales (R3D)** on behalf of a group of Mexican journalists, human rights activists, and students. R3D is appealing the decision to the Inter-American Court of Human Rights.

Data Protection

Data protection laws

The following pieces of legislation concerning data protection have been enacted:

- The **Federal Law on the Protection of Personal Data held by Private Parties** (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, LFPDPPP) enacted on 5 July 2010 and entered into force on 6 July 2010.
- The **Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties** (Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) enacted on 21 December 2011 and entered into force on 22 December 2011.
- The **Privacy Notice Guidelines** (Lineamientos del Aviso de Privacidad) enacted on 17 January 2013 and entered into force on 18 April 2013.
- The **Parameters for Self Regulation Regarding Personal Data** (Parámetros de Autorregulación en materia de Protección de Datos Personales) enacted on 29 May 2014 and entered into force on 30 May 2014.

- The **General Law on the Protection of Personal Data by Public Entities** (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados) entered into force on 26 January 2017.

Accountability mechanisms

According to **the Federal Law for the Protection of Personal Data in the Possession of Private Parties** (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 'LFPDPPP'), the data owners have the right to request access, rectification, and deletion of their personal data, and to object to its processing.

The authority in charge of solving any controversies derived from the exercise of the above-mentioned rights at the federal level is the **National Institute for Transparency, Access to Information and Data Protection** (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 'INAI'). At the local level, each state has its own similar institution. Ultimately, the data owners can also recur to domestic courts through an "amparo", a remedy for the protection of constitutional rights, which is found in certain jurisdictions. The INAI is authorized to perform on-site visits to verify that the data controller's facilities comply with the LFPDPPP. The LFPDPPP provides for the following sanctions:

- A warning instructing the data controller to carry out the actions requested by the data owner, under the terms established by this Law;
- A fine from 100 to 160,000 days of the Mexico City minimum wage;
- A fine from 200 to 320,000 days of the Mexico City minimum wage; and

- In the event of repeated occurrences of the violations described in the preceding paragraphs, an additional fine imposed from 100 to 320,000 days of the current Mexico City minimum wage. With regard to violations committed in processing sensitive data, sanctions may be increased by up to double the established amounts.

Data breaches: case law

Privacy International is not aware of any case law arising from data breach cases in Mexico. Please send any tips or information to: **research@privacyinternational.org**

Examples of data breaches

In 2015, a database containing voter registration records **was published online**, exposing the personal information of 93.4 million Mexican citizens. The records contained the individuals' name, photograph, complete address, date of birth, last names of their parents, occupation and their unique voting credential code. The Instituto Nacional Electoral (INE), a body that oversees the elections in Mexico, **indicated the involvement of a political party** in the leak. The INE later **stated** that it had filed a criminal complaint with Mexico's Special Prosecutor's Office for Electoral Crimes (FEPADE) and the cyber division of the national police.

In 2017, following revelations about a major leak of data from car hire app Uber in 2016, the Mexican National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) **asked Uber for information** on the number of "Mexican users, drivers and employees" that had have been affected. The institute also asked Uber for information on the measures the company is taking to mitigate the damage and protect clients' information.

In October 2017, it was revealed that MoneyBack, the company responsible for returning value-added tax to foreign tourists who visited Mexico, **left an unsecured database on the internet** with 400 GB of files of sensitive personal information, such as passport numbers, credit cards and official IDs of foreign citizens.

Identification Schemes

ID cards and databases

Mexico's national ID card scheme is called the **Unique Population Registry Code** (Clave Única de Registro de Población, 'CURP'). **A CURP number is available** to all inhabitants of Mexico, domestic and foreign, and Mexicans living in other countries. To request a CURP, an individual must provide a copy of an identity document (such as a birth certificate, naturalization letter, or immigration document). **The CURP is currently used in a number of sectors**, including the Tax Administration System (on the Registration of Tax Identification Card, on annual income taxes), education (on school records and certificates) and in military service (on the military service card).

Voter registration

The electoral card ("credencial de elector" or "credencial del INE") is also a widely accepted form of official ID. To obtain an electoral card, a Mexican citizen must present his/her certificate or proof of nationality, photo identification, and a proof of address.

SIM card registration

Mandatory SIM registration was introduced in 2009 in Mexico under the **National Mobile Telephone User Registry** (Registro Nacional de Usuarios de Telefonía Móvil, 'RENAUT') scheme. The scheme **required new subscribers to be fingerprinted** upon purchasing a handset or

phone contract. However, **it was repealed in 2012** and the Federal Institute for Access to Information and Data Protection (IFAI) was required to destroy all personal data of Mexicans contained in the registry.

Policies and Sectoral Initiatives

Cybersecurity policy

In late 2016, the Office of the National Commissioner on Security implemented, by means of the Federal Police, a **Cybersecurity Strategy** that allows the formulation and strengthening of courses of investigation to identify and locate possible perpetrators of cyber attacks. The strategy is carried out by the Scientific Division and has three main premises:

- Preventing cybernetic crimes by disseminating information and orienting citizens;
- Timely detection of cybernetic threats and attacks, with the aim of reducing, neutralizing or mitigating their negative effects on the population; and
- Strengthening the technical and scientific capabilities to investigate and prosecute cybercrime.

In April 2017, the General Secretariat of the Organization of American States (OAS), provided technical assistance to the Mexican government for the development of a National Cybersecurity Strategy.

Cybercrime

In Mexico, there is a **National Response Center for Cybernetic Incidents** (Centro Nacional de Respuesta a Incidentes Cibernéticas, CERT_MX) controlled by the Federal Police. There is also the

Coordination Centre for the Prevention of Electronic Crimes (Coordinación para la Prevención de Delitos Electrónicos) subject to the Scientific Division of the Federal Police.

Encryption

Privacy International is not aware of any laws or regulations that specifically regulate the use of encryption technologies in Mexico. Please send any tips or information to: **research@privacyinternational.org**

Licensing of industry

The telecommunications regulatory body in Mexico is the **Federal Institute of Telecommunications** (Instituto Federal de Telecomunicaciones). The licensing criteria in this field are regulated by:

- The **Federal Law of Telecommunications and Broadcasting**; and
- The **decree that modifies and incorporates** several dispositions to articles 6, 7, 27, 28, 73, 78, 94 and 105 of the Political Constitution of the United Mexican States, in matters of telecommunications.

E-governance/digital agenda

The Mexican government's e-governance initiative, **e-Mexico**, was launched in 2001 following a nationwide consultation process. The **main aims of the initiative** were to increase connectivity through the installation of Digital Community Centers offering low-cost, low-barrier internet access, and create content in various sectors, particularly e-Health, e-Learning, e-Economy, e-Science and Technology, and e-Government.

Health sector and e-health

The Mexican government has an e-Health initiative, **e-Salud**. The portal serves as a clearing house for information related to the physical, mental and social well-being services, health centers and various health promotion and disease prevention and detection tools.

Smart policing

We are not aware of any specific examples of smart policing in Mexico. Please send any tips or information to: **research@privacyinternational.org**

Transport

In 2017, a proposed amendment to the Transportation Law approved by the congress of the Mexican state of Puebla **places obligations on ride-share apps** including Uber and Cabify to provide access to allow "any competent authority" access to clients' data used to provide the service, including GPS data, in order "to monitor the drivers and ensure the safety of users. Mexican civil society group R3D **called on the Puebla Congress** not to approve these amendments to the law over concerns about its vagueness and disproportionality, and the absence of controls and accountability mechanisms governing access to users' data.

Smart cities

In 2016, the Mexican city of Puebla hosted the **Smart City Expo**, a fair of smart city technology and an "international summit of discussion about the link between urban reality and technological revolution." It held another **expo in June 2017**.

Migration

We are not aware of any specific examples of privacy issues related to migration in Mexico. Please send any tips or information to: **research@privacyinternational.org**

Emergency response

We are not aware of any specific examples of privacy issues related to emergency response in Mexico. Please send any tips or information to: **research@privacyinternational.org**

Humanitarian and development programmes

We are not aware of any specific examples of privacy issues related to humanitarian and development programmes in Mexico. Please send any tips or information to: **research@privacyinternational.org**

Social media

We are not aware of any specific examples of privacy issues related to social media in Mexico. Please send any tips or information to: **research@privacyinternational.org**

Location / Region / Locale: Mexico

Programme: Building the Global Privacy Movement

Resource Type: State of Privacy

Type of Intervention: Research

Partner: Red en Defensa de los Derechos Digitales

Advocacy and Policy
Campaigns and Communications
International Network
Investigations and Research
Legal Action
Technical Analysis
Our Impact
Governance
People
Opportunities
Why Privacy?
Financial

Privacy

Why We Use Your Data
How We Use Your Data
How We Learned
Why Cookies?!

Resources

Explainers
Hacking Safeguards
Invisible Manipulation Cases
State of Privacy Briefings
Surveillance Industry Index

Contact Us

62 Britton Street,
London, EC1M 5UY
UK

Charity Registration No: 1147471

Click here to contact us.