Internet surveillance technologies in Mexico

Luis Fernando García
Jesús Robles Maloof

Internews
June 2013

I. Executive Summary

From January to June 2014, a team assembled by researchers Luis Fernando García and Jesús Robles Maloof conducted a research project on Internet surveillance in Mexico as part of a broader effort sponsored by Internews that looked at five countries. During the research period, a telecommunications bill, the establishment of a new regulatory institution, and legal and regulatory reforms were being debated extensively in Mexico. It turned out to be very timely for Mexico to have been included on the list of countries studied.

The researchers had to adapt and monitor the information against the backdrop of a national debate on communications following the introduction of the proposed amendments to the respective regulatory framework to Congress by President Enrique Peña Nieto.

They developed an analysis of the legislation and the relevant decisions that have been handed down by the courts on the issue. They conducted twenty interviews with relevant actors concerning Internet freedom in recent years. They reviewed some of the principal cases of surveillance that were publicized in the media and on the social networks. Finally, they made a number of conclusions.

The study's conclusions include the need to examine communications surveillance within the framework of cooperation between the governments of Mexico and the United States in greater detail. There is significant evidence that the federal government, and some state governments, use surveillance technology against activists and journalists. The study finds that although the case law establishes criteria favoring privacy, significant impact litigation is needed to ensure their application.

Future research into the role of state and municipal governments in the surveillance of communications is necessary given the vagueness of the relevant provisions, the limited legal and political oversight to which those governments are subject, and the extremely broad range of authorities to be studied.

II. Introduction

In recent years, the surveillance conducted by States and their capabilities relative to surveillance technologies took center stage in international debates on freedom of expression, privacy, and democracy. The revelations of Edward Snowden in 2013 were an important inflection point for civil society throughout the world, and sparked an international movement that called for a debate on the very roots of democracy.

One of the initial lessons of this inflection point is that granting surveillance powers to the authorities without an adequate legal framework, without independent institutions, and without an accountability process, will invariably lead to abuses. In the space of a few short years, the NSA went from monitoring terrorist activities to spying on its country's own citizens, the presidents of democratic countries, and leaders considered allies, including Felipe Calderón and

Enrique Peña Nieto.[1]

Mexico is at the epicenter of this debate, in principle because of the role it plays as a strategic ally of the United States, and also because of the societal violence of recent years that has caused the security budgets of the federal, state, and municipal governments to multiply year after year. A good part of this budget has been earmarked for surveillance technology to monitor telecommunications, public areas, and the borders, among other parts of society. However, the results of this investment are no t entirely clear.

Given the current legal regulations on the issue, we can assert, at least hypothetically, that certain surveillance acts—although considered lawful—create uncertainty about the observance of the fundamental rights to privacy and freedom of expression because of the breadth of the laws, their ambiguity, the insufficient regulation of the surveillance powers, and their overlap with a complex system of concurrent powers.

At the outset, the use of technologies for the consolidation of the rule of law seems positive. However, the justification for the increased use of technology in the hands of governments does not take account of government corruption, nor does it eradicate impunity—much less go to the root of the crime. We must confront the violence of organized crime with the best technical means, but this—without exception—must be done under the principles of due process, by means of a crime policy based on administering justice and with social policies that put an end to exclusion.

The following is our initial approach to State surveillance and the social perception thereof.

1 http://mexico.cnn.com/nacional/2013/10/20/la-nsa-espio-el-correo-de-felipe-calderon-revelo-der-spiegel

III. Background

2013 has been marked by the introduction of legislative bills seeking to control and restrict social protest and curtail the exercise of freedom of expression and association. These legal initiatives include proposed amendments to Article 362 of the Criminal Code in Mexico City and to the National Code of Criminal Procedure in the Federal Congress, the laws on public demonstrations proposed in Jalisco, San Luis Potosí, and Mexico City, and those enacted in Quintana Roo and in Chiapas and Quintana Roo.

The digital side of this trend toward control has been a set of proposals at the federal and local levels that seek to establish a policy of surveillance inconsistent with the international standards on freedom of expression. The ruling party in government has been characterized in the past by its control over political decisions and has adapted to the times of the so-called transition to democracy by using devices including legislative pacts to create the impression of political legitimacy in a democracy whose institutions are often called into question.

The key is not so much in making radical changes to the political methods, but rather in adapting them to the current circumstances. A central part of this strategy entails keeping an iron grip on the media and silencing critical voices, including those on the Internet, in order to clamp down on freedom of expression. At this juncture, the governments of the states where there is the least legislative, judicial, or citizen oversight have reinforced their control over local public opinion by all kinds of methods ranging from the purchase of advertising to threats and even physical assaults.

At the same time, the government is engaged in intense national and international communication-related activity concerning freedom of expression, including digital rights activism, such as Mexico’s participation in the Freedom

Coalition Online[2] and the promotion of declarations on privacy in the Internet age at the United Nations General Assembly.[3]

During the past year a number of surveys were conducted in Mexico on the perception of surveillance. In particular, the polling agency Parametría took national telephone surveys on the following issues: “Mexicans believe that U.S. spying will continue” (November 2013)[4] and “Mexicans condemn government spying” (July 2013).[5] Both surveys underscore the public’s general unease over news on government spying, but also reflect the perception that it will continue. We will examine the survey that was conducted for this research project below.

IV. Overview of Surveillance Policies and Regulations in Mexico

Over the past five years, the laws, surveillance regulations, and the national budget[6] in Mexico have undergone drastic changes. Against the backdrop of the so-called “war on organized crime,” and spurred on by international cooperation agreements on security such as the “Mérida Initiative,” Mexico has undertaken a series of legal reforms that provide for an increase in the surveillance powers and techniques available to the security agencies, whether for the investigation and prosecution of crimes or to prevent national security threats.

Right to Privacy of Communications in Mexico

The privacy of communications is generally protected by Article 16 of the constitution, paragraphs 12 and 13 of which establish that private communications are inviolable, that only a federal judge can authorize the surveillance of private communications at the request of an authority, and that

2 http://www.freedomonline.ee/about-us/member-states
3 http://www.un.org/es/comun/docs/?symbol=A/RES/68/167
4 http://www.parametria.com.mx/carta_parametrica.php?cp=4616
5 http://www.parametria.com.mx/carta_parametrica.php?cp=4561
6 Violence and the use of budgets for security:
http://www.asf.gob.mx/uploads/74_Mensajes_del_Titular/Seguridad_Colmex.pdf , Mexico 2014

the type of surveillance, the subjects of the surveillance, and its duration must be specified.

The Mexican Supreme Court has established that the protection of private communications includes all existing forms of communication, including those that are the result of technological advances.[7] Therefore, it is clear that private communications on the Internet are constitutionally protected in Mexico.

In addition, both the Supreme Court and the Inter-American Court of Human Rights, whose case law is binding on all judges in Mexico, have acknowledged that the right to the inviolability of private communications protects not only the content of the communications but also the data that identify the communication, or "communications traffic data," such as the identity of the parties to the communication, the duration of the communication, geographic location, and the identification of an Internet protocol address (IP address).[8]

The Supreme Court has also ruled that private communications are constitutionally protected from real-time surveillance, as well as from subsequent interference with the hardware on which the communication is stored.[9]

Regulation of the Surveillance of Private Communications

At the federal level, there are multiple authorities that have the power to request the surveillance of private communications. The Office of the Attorney General of the Republic (PGR) has such power pursuant to the Federal Code of Criminal Procedure, which was amended in 2009 for that purpose.[10] In addition, the

7 Supreme Court of Mexico. First Chamber. Review of Petition for Constitutional Remedy [*Amparo*] 1621/2010 & Judgment 194/2012.

8 Supreme Court of Mexico. First Chamber. Review of Petition for Constitutional Remedy [*Amparo*] 1621/2010 & Judgment 194/2012; Inter-American Court of Human Rights. Case of Escher et al. v. Brazil. Preliminary Objections, Merits, Reparations, and Costs. Judgment of July 6, 2009. Series C No. 200.

9 Supreme Court of Mexico. First Chamber. Review of Petition for Constitutional Remedy [Amparo] 1621/2010 & Judgment 194/2012.

10 Federal Code of Criminal Procedure. Arts. 278 *Bis* & 278 *Ter.*

kidnapping laws of 2010[11] and organized crime laws of 2007[12] give the PGR the ability to eavesdrop on private communications. The state public prosecutors' offices also usually have the authority to monitor private communications under state law.

Additionally, the Federal Police Act, which was passed in 2009, authorizes the police to intercept private communications for the prevention of certain criminal offenses.[13]

The National Security Act also grants the National Security and Investigation Center [*Centro de Investigación y Seguridad Nacional*] (CISEN) the authority to intercept private communications in cases of "imminent threat to national security."[14]

On the issue of surveillance, the National Public Security System Act authorizes all police agencies to conduct information-gathering activities through "standardized systems."[15] Finally, the federal, state, and even municipal laws contain provisions for the blocking, restriction, or surveillance of communications in detention centers.

The above-cited laws include Internet communications among those communications subject to interception pursuant to a warrant from a federal judge. Those laws do not establish any other safeguards against abuse, such as supervision by an independent body, statistical transparency requirements, or subsequent notice to the person affected by a surveillance measure.

Recent Amendments

11 General Law to Prevent and Punish Crimes of Kidnapping. Articles 24 & 25
12 Federal Law on Organized Crime. Arts. 8 & 16-28.
13 Federal Police Act. Arts. 48-55.
14 National Security Act. Arts. 33-49.
15 National Public Security System Act. Arts. 30 & 35, *inter alia.*

In 2009, the Federal Telecommunications Act[16] was amended to require that telecommunications service providers keep communications traffic data (metadata) including communication type, services used, origin and destination of communications, date, time, and duration of the communications, and even the geographic location of communications devices. The obligation to maintain the data lasts for twelve months, and it applies to all users of services provided by the telecommunications companies.

The Federal Telecommunications Act allows the Office of the Attorney General and the state prosecutors' offices to access the data held by the telecommunication companies for the investigation of serious criminal offenses without the need to obtain a judicial warrant.

In 2012, the Federal Telecommunications Act[17] was again amended to establish the obligation of telecommunication companies to cooperate with the Office of the Attorney General and the state prosecutors' offices to provide the geographic location, in real time, of mobile communication devices without the need for a judicial warrant or any other safeguard.

The National Code of Criminal Procedure, which will replace the Federal Code of Criminal Procedure and the 32 State Codes, was published in March 2014. The new Code, which will take effect in stages and be in full force by June 2016, reiterates the surveillance powers of the prosecution authorities. One important advance is that this Code does require judicial authorization for the interception of all types of communications, including metadata, whether in real time or for their retention.

Nevertheless, the possibility remains in this new Code for the warrantless monitoring of the geographic location of communication devices in real time, and it allows for the retention of data contained in networks, systems, or computer

16 Federal Telecommunications Act. Art. 44 §§ XII & XIII.
17 Federal Telecommunications Act. Art. 40 *Bis*.

equipment to be ordered without a judicial warrant. The Code also fails to add adequate safeguards such as independent oversight, statistical transparency measures, or mechanisms for providing deferred notice to affected users.

Finally, in March 2014 the Federal Government introduced a new Telecommunications and Broadcasting bill[18] that includes the broadening of surveillance measures. Accordingly, the bill increases the data retention period to 24 months, and even allows for data to be kept indefinitely at the mere request of a government authority.

The bill would also allow authorities outside the criminal justice system, such as the National Security and Investigation Center, the Army, the Navy, and the Federal Police, to ascertain the geographic location of mobile communication devices in real time and to access the data retained by the telecommunication companies without having to secure a warrant from a federal judge, on the broad and vague premise of "the exercise of the powers inherent in the production of intelligence." At the time of this writing, the debate and vote on this bill, scheduled for April 2014, had reportedly been postponed because of significant opposition to those provisions.

V. Events related to surveillance

There has been a history of Internet censorship, repression, and surveillance by governments from the time activists and journalists started using the web in the 1990s. Nevertheless, we can point to 2010 as the year that ushered in a phase of systematic government surveillance and the critical opinion of Internet users due to the increased number of users and to the increased use of social media as a forum for public debate.

The following are some relevant examples reported by the mainstream media:

18 Draft bill of the Federal Telecommunications and Broadcasting Act and the Mexican Public Broadcasting System Law, Arts. 189-197. Available at:
http://www.presidencia.gob.mx/wp-content/uploads/2014/03/INICIATIVA-LEY-CONVERGENTE.pdf

Arrest of Héctor Bautista in Chiapas. 2010.

In November 2010 Héctor Bautista, a member of the free software community and administrator of the InfoChiapas.com network, was arrested by state police in the State of Chiapas on trumped-up child pornography charges.[19] The cyber-police participated in his arrest and seized his computer equipment and memory cards.

The real motive for his arrest was the publication of an article by journalist Antony Flores on the state government's debt that had been dismissed by the mainstream media and published on InfoChiapas.com. After 40 days in custody and a national campaign for his release, Héctor was set free. The case received very little coverage in the mainstream media, but a television news report[20] helped raise awareness of the censorship and criminalization that the case represented. Héctor Bautista went back to his work and continued to be part of the community of free software bloggers in Chiapas. The laws at issue in this case were mainly the Criminal Code of Chiapas and the *Amparo* Act.

The "Terrorist Tweeters" of Veracruz. 2011.

On August 25, 2011, in the port of Veracruz, scenes of panic took place at most of the city's elementary schools. Thousands of parents returned to the schools to pick up their children just a few hours after having dropped them off. The rumor was that there was an organized crime attack on schools. That afternoon, the state prosecutor asserted that the panic was a concerted provocation by a "group" of "terrorists" who were being investigated and arrested.[21] Technical means at the disposal of the cyber-police were used to arrest Twitter and Facebook users Maruchi Bravo and Gilberto Martínez.

19 http://censura-chiapas.blogspot.mx/search?updated-max=2010-11-15T09:12:00-08:00&max-results=7
20 http://censura-chiapas.blogspot.mx/2010/12/punto-de-partida-denise-maerker-un.html
21 http://www.youtube.com/watch?v=Hzlsf-Z1m1c

They were arrested and prosecuted for the crime of terrorism, which carries a maximum sentence of 30 years. As documented in the case, it was found that the panic in that city had started even before the messages of both users who, hours later, merely commented on what was being heard in the streets.[22] It was found that the government of Veracruz was seeking to create guilty parties and criminalize the use of social networks. The case gave rise to an important campaign of journalists and Internet users. In an attempt to silence the critics, the government and congress amended the law to try to minimize the potential sentence. In 2013, the Supreme Court of Mexico finally ruled that the amendment was unconstitutional, setting an important precedent.[23] Maruchi and Gilberto regained their freedom after the case was dismissed by the government and they are now digital activists. The relevant laws in this case were the Criminal Code of the State of Veracruz, the *Amparo* Act, and the Constitution with regard to the constitutional challenge.

Facebook users arrested, tortured, and prosecuted for announcing #OP5Puebla. 2013.

On May 3, 2013, Iván Guizasola Vázquez, Néstor López Espinosa, and Eduardo Salazar Velázquez were arrested after calling for a protest for May 5, 2013 called #OpPuebla via Facebook. The newspaper Cambio, citing government sources, published on Saturday, May 4 that the state prosecutor's office had dismantled the foolhardy attempt to "attack the presidential motorcade."

The Facebook event #OpPuebla was cancelled at 23:45 hours on Saturday, and there was no protest on May 5. Groups of more than twenty people in civilian attire intercepted the men in different places on Friday May 3, without identifying themselves or displaying a judicial warrant, and took them to a still-unidentified location for interrogations that involved torture methods. On Friday afternoon, investigative police searched their homes, and in the case of Eduardo, his mother's

22 http://latimesblogs.latimes.com/laplaza/2011/09/twitter-mexico-veracruz-details-confusion-rumor-precedents.html?dlvrit=99665

23 http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=132774

stationery store and Internet café. The abuse included multiple beatings and mock hangings. The police placed hoods over the men's heads and held cocked weapons to their temples and ribs.

The three Facebook users were released from custody a week after their arrest, but are still being prosecuted for various criminal offenses.

Gustavo Maldonado, blogger arrested in Chiapas. 2013.

Gustavo Maldonado was accused of small-scale drug dealing,[24] and arrested on August 8, 2013,[25] in a case that was plagued with irregularities. The only evidence was an anonymous complaint and the testimony of the investigative police. No physical evidence of the alleged illegal substance was presented. The authorities used molecular detector[26] GT – 200,[27] whose British manufacturers are in prison for promoting this device because it in fact does not detect anything. Although Maldonado had reserved his right to make a statement, the prosecutor asked him "special questions" that were later taken as confessions (the Supreme Court has ruled them unconstitutional).

In point of fact, Gustavo is a critic of the governments in Chiapas, and in recent months he had called for demonstrations on the issue of water in Tuxtla Gutiérrez, among other causes he supported. The afternoon of his arrest, he released a video and re-tweeted information about the purchase of the "Blackeyed Hosting Monitor,"[28] surveillance equipment for locating digital activists in Chiapas. On the night of August 8 of this year, he was arrested while buying dinner.

Gustavo Maldonado was released after ninety days in jail and is currently awaiting a decision in his case.[29]

24 http://www.proceso.com.mx/?p=349780
25 http://www.pgje.chiapas.gob.mx/prensa/Articulo.aspx?id_articulo=71E06C4F-6967-4237-AF40-1C3A9BCEBAF2
26 http://em.fis.unam.mx/blog?-tags=gt200
27 http://www.sinembargo.mx/opinion/01-10-2013/17907
28 https://twitter.com/gumalo3105/status/365673957984186370
29 http://www.proceso.com.mx/?p=357382

Harassment of journalist Lydia Cacho and falsification of news websites. 2013

In September, journalist Lydia Cacho published an article entitled “State Cyberterrorism”[30] in which she reported various acts of harassment by an organization allegedly linked to the party in power. The piece recounts actions to be taken against the journalist and the techniques whereby false opinion is created on social media in favor of state governors, in particular, Roberto Borge of Quintana Roo. The falsification consists of counterfeiting news images from the newspapers Reforma and Sin Embargo in order to disseminate them as real.

It is not known whether the journalist has taken any legal action.

Censorship of 1dmx.org

1dmx.org is a website that served as a platform for the dissemination of evidence of human rights violations that occurred during the protests over the inauguration of the current president, Enrique Peña Nieto, on December 1, 2012.

On December 2, 2013, the U.S. company GoDaddy.com informed the administrators of 1dmx.org of the suspension of their domain name. On December 3, GoDaddy.com reported via email that the suspension of the domain was part of an ongoing police investigation, and that for more information they should contact a national security officer at the Embassy of the United States in Mexico.[31]

The attorneys for 1dmx.org filed a lawsuit against Mexican agencies suspected of requesting the suspension of the website through the Embassy of the United States in Mexico; however, all of them have denied doing so. The United States

30 http://www.sinembargo.mx/opinion/12-09-2013/17347

31 http://www.animalpolitico.com/2014/03/acusan-comision-de-seguridad-y-embajada-de-eu-de-censurar-pagina-web-del-1dmx/#axzz34lFM1Csh

government has refused to provide any information. For its part, GoDaddy.com informed 1dmx.org's attorneys via telephone that the agency responsible for the original request was the Specialized Technology Response Center (CERT), a division of the National Security Commission (CNS – Federal Police) under the Federal Ministry of the Interior.

On March 4, 2014, 1dmx.org made the case public. In less than 24 hours the domain was restored without explanation.[32] GoDaddy.com reported weeks later that the reinstatement was due to the fact that it had been informed that the investigation giving rise to the suspension had been deactivated, and it again referred the administrators to the United States embassy and the Mexican government for further information. At this point, neither government has agreed to provide information.

Acquisition and use of surveillance equipment by the Mexican government. 2007 – 2014.

There have been reports since 2007 of the Mexican government's cooperation with the U.S. government to tap telephone calls and emails with equipment made by the Verint company provided to the Mexican government with the ability to intercept up to 3 million communications. "It is a government of Mexico operation funded by the U.S.," said Susan Pittman, of the State Department's Bureau of International Narcotics and Law Enforcement Affairs in statements to the L.A. Times in 2007.[33] In 2011, Mexican officials denied the operation of U.S. agents, but confirmed that there was cooperation in the exchange of information.[34]

In 2012 it came to light that the National Defense Department had contracts to acquire communications surveillance and intercept equipment with the capacity to conduct email monitoring and voice interception, intercept ambient

32 http://www.animalpolitico.com/2014/03/restablecen-sin-explicacion-sitio-de-1dmx/#axzz34lFM1Csh
33 http://articles.latimes.com/2007/may/25/world/fg-mexico25
34 http://www.jornada.unam.mx/2011/08/18/politica/005n1pol

background noise, capture images, extract SMS and MMS, contact lists, calendar records, GPS location, and screen shots, access and manipulate file systems, SIM card information, hardware information, and mount denial of service attacks.[35]

In January 2013, the University of Toronto's Citizen Lab program publicized the existence in various countries, including Mexico, of the surveillance software Finfisher from Gamma International. The software is meant for law enforcement and security agencies, but has been used by governments in documented cases to eavesdrop on the communications of activists, journalists, and rights defenders.[36] Civil society organizations in Mexico filed a request for investigation with the personal data protection authority[37] and called upon the government to publicly disclose its acquisition of surveillance equipment and the protocols used. The case remains under investigation.

In July 2013, the web portal Impacto published part of the contracts entered into by the Office of the Attorney General to acquire equipment and user licenses for the surveillance software "Plint Tracking Locsys" and "Hunter." The purpose of these contracts is to have the technology to locate communication devices in real time.[38] That month, Citizen Lab publicized the operation of Blue Coat network surveillance software in Mexico, Mexico being second only to the United States in the amount of equipment detected.[39]

That same year, the existence of the surveillance and spyware equipment contracts that are part of the aforementioned 2007 agreement between the U.S. and Mexican governments was confirmed, and documents relating to those contracts came to light.[40]

35 http://aristeguinoticias.com/1607/mexico/a-detalle-los-5-contratos-de-sedena-para-espionaje-de-celulares-y-radios/
36 https://citizenlab.org/2013/04/for-their-eyes-only-2/
37 http://contingentemx.net/2013/10/07/comunicado-de-prensa-sobre-los-avances-en-las-investigaciones-sobre-finfisher-en-mexico/
38 http://impacto.mx/opinion/oAq/impacto-documenta-adquisici%C3%B3n-de-equipo-de-espionaje-de-pgr
39 https://citizenlab.org/2013/07/planet-blue-coat-redux/
40 https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=61908be80b65585671594e1fd11525e0&_cview=1

In January 2014, Citizen Lab reported the use of “Da Vinci” surveillance software made by the company Hacking Team in various countries including Mexico, and noted that it has been used in other countries against activists and journalists.[41]

Table on mentions in the media

Sources Used	**Keywords**	**How Many Events**
Reforma.com (Number of articles containing these words published in the national section since 1993.)	Internet censorship	57
	Twitter censorship	9
	Social networks surveillance	57
	Communications surveillance equipment	64
	Communications spying	191
La Jornada (Number of articles containing these words published in the national section since 1996, using the search engine Google)	Internet censorship Mexico	286
	Twitter censorship Mexico	911
	Social networks surveillance Mexico	1,160
	Communications surveillance equipment Mexico	677
	Communications spying	336
Twitter	Twitter censored Mexico	1,000

41 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

(Using the tool Topsy)	Facebook censored Mexico	20
	Surveillance social networks Mexico	1,000
	Spying social networks Mexico	800
	Twitter user arrested	800

VI. Perceptions regarding surveillance

Description of Profiles

A: Journalist specializing in social issues and national and state politics in the State of Quintana Roo, between 20 and 30 years of age.

B: Digital activist and developer of web pages on social movements in Mexico City, between 29 and 39 years of age.

C: Social activist and founder of a human rights defense organization in Mexico City, between 49 and 59 years of age.

D: Freelance journalist in the State of Puebla specializing in accountability issues, between 29 and 39 years of age.

E: Digital activist in the State of Veracruz monitoring issues concerning Internet freedom, between 39 and 49 years of age.

F: Digital activist in the State of Chiapas who is a participant in social movements and a critic of government practices, between 29 and 39 years of age.

G: Human rights defender in the State of Chihuahua specializing in information technology, between 29 and 39 years of age.

H: Human rights defender specializing in women's rights in the State of Chihuahua, between 29 and 39 years of age.

I: Student and user of social networks in the State of Puebla, between 21 and 29 years of age.

J: Academic and researcher on social movements and the Internet in Mexico City, between 39 and 49 years of age.

K: Social activist in Mexico City, participant in social protests, between 39 and 49 years of age.

L: Human rights defender in the State of Quintana Roo. Litigates public interest cases. Is between 29 and 39 years of age.

M: Journalist specializing in accountability in Mexico City, between 29 and 39 years of age.

N: Digital activist in the State of Morelos. Participates in networks for the search for missing persons. Is between 29 and 39 years of age.

O: Social activist in the State of Morelos and in Mexico City, between 21 and 29 years of age.

P: Was a student activist in Mexico City and now works at a civil society organization. Is between 21 and 29 years of age.

Q: Was a student activist in Mexico City and continues to be a social activist. Is between 21 and 29 years of age.

R: Member of a collective and independent media outlet based in Mexico City that documents social movements. Is between 21 and 29 years of age.

S: Lawyer. Works at a human rights defense organization in Mexico. Is between 21 and 29 years of age.

O: Is a social activist in the State of Morelos and in Mexico City, between 21 and 29 years of age.

P: Was a student activist in Mexico City and now works at a civil society organization. Is between 21 and 29 years of age.

Q: Was a student activist in Mexico City and continues to be a social activist. Is between 21 and 29 years of age.

R: Member of a collective and independent media outlet based in Mexico City that documents social movements. Is between 21 and 29 years of age.

S: Lawyer. Works at a human rights defense organization in Mexico. Is between 21 and 29 years of age.

General perceptions on government surveillance

Most of the interviewees (79%) said that they were aware of some kind of government surveillance. Nevertheless, the depth of their awareness is highly variable. The state surveillance techniques, programs, or measures mentioned by the interviewees include: The interception of private communications and real-time geolocation of mobile communication devices (63%); the use of malicious

spyware such as FinFisher and Keyloggers (42%); the purchase of surveillance equipment by the State (26%); use of surveillance cameras (11%); online harassment of persons of interest (11%); monitoring of the public activities of persons of interest (5%), and access to Internet users' data (5%).

The interviewees based their general knowledge of government surveillance measures on information obtained through: Internet media (63%); social networks (47%); print media (37%); reports from organizations (42%); word of mouth (37%); and radio and television (26%). Independently of specific knowledge of state surveillance programs, techniques, or events, all of the interviewees hold the opinion that government surveillance has increased in recent years.

Nearly all of the interviewees (95%) suspect that they are or have been the victim of government surveillance. Nevertheless, the level of evidence presented is highly variable. Thirty-two percent of the interviewees failed to cite specific evidence that would lead to the conclusion that they have been subject to government spying. Twenty-six percent mentioned the faulty operation and strange behavior of communication equipment as the reason for their suspicions. Twenty-one percent mentioned acts of harassment and intimidation. Sixteen percent of the interviewees cited the hacking of email accounts as an indication of surveillance. Sixteen percent also mentioned cyberattacks on their servers and websites as evidence of surveillance. In addition, 16% suspect that they are being spied on due to the fact that, for example, members of the group have been contacted by government agents or have received anonymous threats through email accounts and telephone numbers that have not been made public.

In some cases, the alleged evidence is more substantial. For example, one of the interviewees claims to be able to prove the detection of the malware FinFisher on his/her equipment, in addition to various acts of harassment. Another interviewee mentioned the detection of an agent who had infiltrated the online group. On one

occasion it was mentioned that a state agent had confirmed to one of the interviewees that he/she was under surveillance.

It was mentioned in one of the interviews that a significant number of the group's members had their cell phones stolen in isolated incidents that occurred during a short period of time, raising the suspicion that the thefts were motivated by their work and the intent to monitor other members of the group.

One of the interviewees even reported that at the peak of his/her political involvement in a student movement, university authorities showed him/her private Facebook conversations that the authorities themselves revealed had been obtained by the Presidential General Staff, which would indicate that this agency has access to private online conversations.

Various interviewees have had their suspicions reinforced by experiencing one or several of the abovementioned events specifically during periods in which their professional work of political participation has created unusual public attention or has affected the interests of some political group or government agency.

Eighty-four percent of the interviewees believe that surveillance is used by the State to intimidate them because of their professional work, political participation, or activism. The same percentage of interviewees considers it highly likely that the surveillance extends to their personal lives.

Effects of surveillance on behavior

Seventy-nine percent of the interviewees have modified their behavior based on the suspicion or threat of being subject to surveillance. Sixty-eight percent of the interviewees have changed the way in which they interact online to avoid sharing sensitive information by technological means or instead prefer to discuss sensitive matters in person. Sixteen percent have changed habits pertaining to their

passwords. Eleven percent have adopted comprehensive security protocols within their organizations.

Use of anti-surveillance measures

All of the interviewees mentioned being aware of the existence of technological means to counteract the surveillance of their communications. Nevertheless, 26% of the interviewees do not know of any specific measure. Forty-two percent mentioned TOR. Twenty-six percent specifically mentioned email encryption. Twenty-one percent cited email services such as Hushmail, Safemail, and Riseup Mail, which the interviewees perceived to be safer. Twenty-one percent made reference to the messaging service Kik. Eleven percent mentioned being familiar with the tools contained on the “Security in a Box” platform. One of the interviewees also referenced the installation of privacy add-ons to his/her browser and the frequent use of antivirus software as measures to counteract surveillance.

In spite of their knowledge of measures to counteract surveillance, only 42% use any such measures. Sixteen percent use TOR. Twenty-one percent use Kik Messenger. Twenty-one percent use email services such as Hushmail, Safemail, or Riseup Mail. Only 5% use email encryption keys. One person uses privacy add-ons on his/her browser and frequently uses antivirus software.

The biggest obstacle to the use of anti-surveillance measures expressed by the interviewees is complexity or the lack of knowledge or ability to use such measures (84%). One group of interviewees (21%) believes that taking technological measures to counteract surveillance could be an exaggerated response to a threat that is not perceived as being serious enough to warrant such steps. Eleven percent think it is difficult to take measures if they are not taken together with others with whom they communicate. Finally, 5% of the interviewees expressed mistrust of the effectiveness of the measures, and the same number even expressed their concern that the use of anti-surveillance measures would place them at an increased risk.

Notwithstanding the above, all of the interviewees affirmed that they would like to use measures to counteract surveillance if those measures overcome the obstacles identified.

IV. Conclusions

The research was conducted in the context of extensive debate on communications and the role of the State in communications surveillance, given the discussion in Congress of the amendments to the regulatory framework—which was a challenge in view of the information available.

Mexico is a federal republic, and the research demonstrated the resulting complexity of examining the regulatory framework given the concurrent public security powers of the federal government, states, and municipalities, and the ambiguity of the laws on the subject. Future research on the legal framework, related cases, and the perception of communications in each one of the 32 states and in the municipalities that conduct surveillance tasks is needed in order to have a more precise overview of what surveillance represents.

The proximity and the extensive cooperation between the Mexican and U.S. governments in the surveillance and interception of communications calls for more specific research on its scope, the legal framework that supports it, the oversight to which this activity is subject, and the outcome of these activities.

The Mexican regulatory climate surrounding communications surveillance—particularly on the Internet—has evolved in recent years because of the context of violence and insecurity, and because of international cooperation agreements on security such as “the Mérida Initiative.” As such, the surveillance powers of law enforcement and national security authorities have increased significantly,

without the simultaneous establishment of institutional checks and balances to decrease the risk of surveillance authority being abused.

There is very limited statistical data on the use of surveillance measures, which makes it difficult to accurately assess their effectiveness or to measure their scale and the risks associated with this type of surveillance. There is scant information on the techniques, equipment, and budgets earmarked for surveillance activities. The absence of information makes it hard to counteract the narrative that is driving the increase in surveillance powers on the unproven premise that such measures contribute to the accomplishment of legitimate aims such as national security or public safety.

As the research suggests, activists, journalists, and human rights defenders all possess a superficial knowledge of the State's surveillance powers and measures. In addition, the media—principally the mainstream media—do not appear to pay frequent attention to matters related to surveillance.

In spite of the above, the information obtained through the research has made it possible to document that there is a high presumption that surveillance measures are used for political purposes against certain groups. Although the suspicions of surveillance are not supported by evidence in every case, there are significant indicia that surveillance measures are used against human rights defenders, activists, and journalists.

Irrespective of the above, the threat of surveillance has led to changes in the behavior of a significant number of people. This effect alone is of concern, as it inhibits—or at least hinders—the exercise of rights such as freedom of expression, association, and human rights defense. Nevertheless, although there is great interest in taking measures to counteract the threat of surveillance, the research suggests that there is little knowledge of anti-surveillance technological measures.

The main obstacle to the adoption of technological measures against surveillance is the perceived complexity of their implementation. Accordingly, greater efforts must be made to develop tools that are adapted to local contexts and that are easy to adopt, in order to satisfy the demand for these kinds of tools and to limit the detrimental effects of the perceived threat of surveillance. This is especially the case when that perception is accompanied by a feeling of defenselessness, which can lead to the normalization of the state of perpetual surveillance and the erosion of rights.

In addition, the lack of oversight and safeguards such as judicial review, independent supervisory bodies, statistical transparency measures, or deferred notice to the affected party poses serious risks to the public, especially to human rights defenders, activists, and journalists, as it allows the authorities to engage in serious invasions of individual privacy with the knowledge that the use of that power can be kept secret in perpetuity, without any need for accountability. This scenario makes it necessary to redouble efforts to document the use of surveillance powers in Mexico in greater detail.

Moreover, although there is a constitutional and human rights framework that has been interpreted in favor of the right to privacy in some judicial precedents, the need remains for the judicial branch to consolidate its emerging doctrine on the right to privacy in cases that involve covert surveillance programs. The use of impact litigation may be essential in the advancement of this right, especially in view of the recent passage of legal reforms that increase surveillance powers without establishing safeguards.

The consolidation of high standards on the protection of the right to privacy vis-à-vis covert surveillance measures can at the same time inform legislation and surveillance practices that are compatible with human rights.